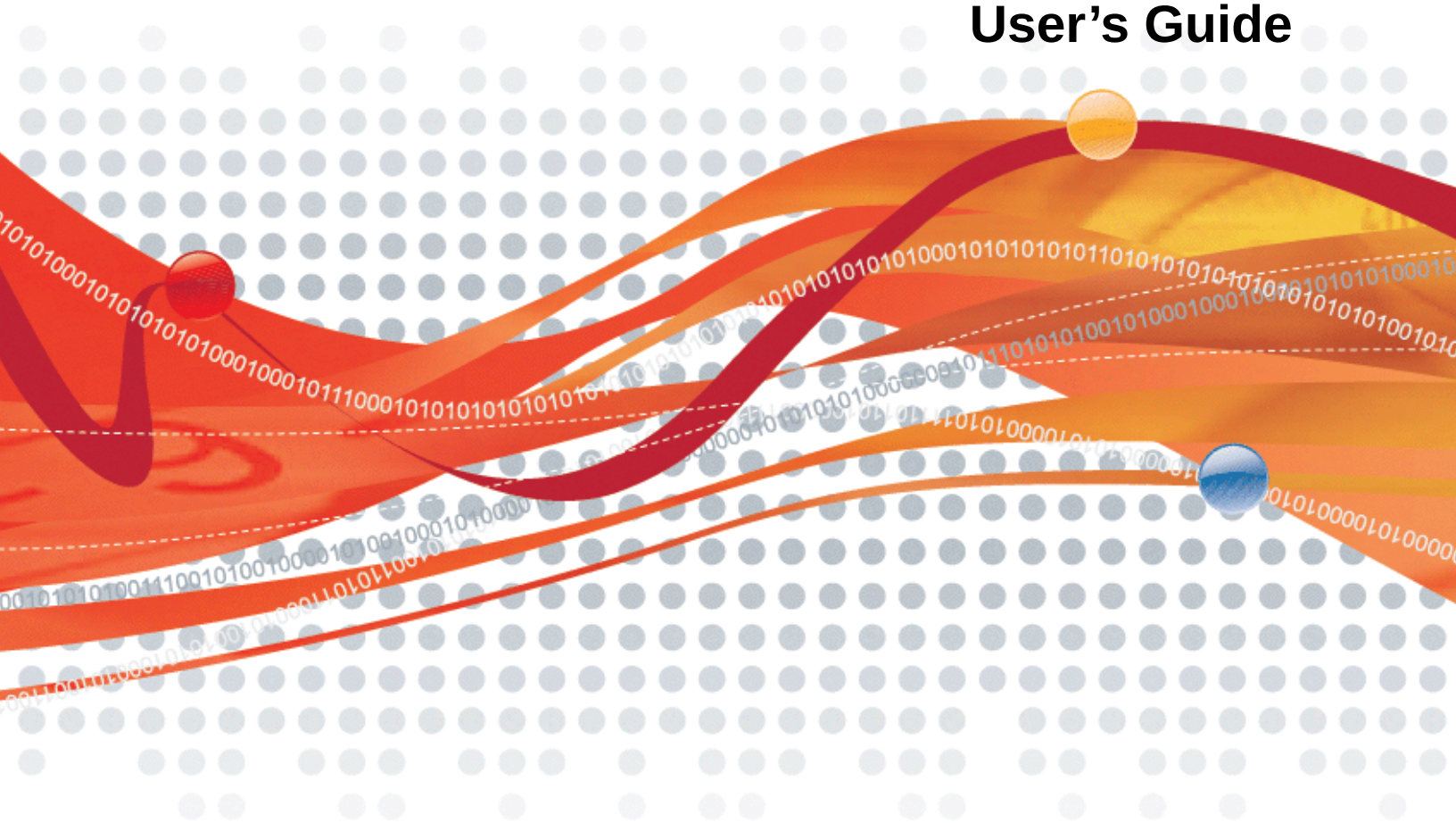
TREND MICRO™

Deep Security 7.5

User's Guide



Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

http://www.trendmicro.com/download

Trend Micro, the Trend Micro t-ball logo, OfficeScan, Intrusion Defense Firewall, Control Server Plug-in, Damage Cleanup Services, eServer Plug-in, InterScan, Network VirusWall, ScanMail, ServerProtect, and TrendLabs are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2011 Trend Micro Incorporated. All rights reserved.

Document number: APEM74807/110302
Document version: 1.2
Release date: March 2011

Table of Contents

How this document is organized 5

Deep Security 7.5 6

What's New in Deep Security 7.5 10

Deep Security Manager Interface 11
Dashboard 15
Alerts 17
Reports 18
Computers 19
  Computer Details 28
Security Profiles 35
  Security Profile Details 36
Anti-Malware 41
  Anti-Malware Events 42
  Quarantined Files 44
  Anti-Malware Configuration 46
Firewall 49
  Firewall Events 50
  Firewall Rules 53
  Stateful Configurations 56
Deep Packet Inspection 60
  DPI Events 61
  DPI Rules 63
  Application Types 66
Integrity Monitoring 68
  Integrity Monitoring Events 69
  Integrity Monitoring Rules 71
Log Inspection 74
  Log Inspection Events 75
  Log Inspection Rules 77
  Log Inspection Decoders 79
Components 80
  Directory Lists 81
  File Lists 82
  File Extension Lists 83
  IP Lists 84
  MAC Lists 85
  Port Lists 86
  Contexts 87
  Schedules 89
System 90
  System Events 91
  System Settings 93
    Computers 94
    Anti-Malware 97
    Firewall and DPI 98
    Integrity Monitoring 102
    Log Inspection 103
    Interface Isolation 104
    Contexts 105
    Reconnaissance 106
    Scan 108
    Notifications 109
    Ranking 111
    System Events 112

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Security 113
Updates 114
System 115
System Information 117
Tags 120
Tasks 121
Roles 123
Users ..... **Error! Bookmark not defined.**
Contacts 129
License 130
Updates 131

The Deep Security Virtual Appliance Interface 134

How To 135
Add Computers to the Manager 137
Configure Alerts 140
Configure Logging 141
Configure Manager to Agent/Appliance Communications 142
Configure Notifications 144
Configure Port Scan Settings 145
Configure Syslog Integration 146
Customize the Dashboard 157
Export or Back Up Data 160
Filter SSL Data Streams 163
Manually Deactivate/Stop/Start the Agent/Appliance 167
Secure the Deep Security Manager 168
Set Up Email Alerts 169

Reference 170
About Firewall Rules 173
Advanced Logging Policy Modes 177
Agent/Appliance Events 179
Bypass Rule 185
Computer and Agent/Appliance Status 186
Creating Custom DPI Rules 190
Creating Custom Log Inspection Rules 200
Creating and Applying New Firewall Rules 216
DPI Events 218
Disabling Diffie-Hellman in Apache 220
Encrypting DSM to DB Communication 221
Event Tagging 222
Firewall Events 224
Firewall Rule Sequence 226
Inheritance and Overrides 227
Integrity Monitoring Rules Language 232
DirectorySet 242
FileSet 244
GroupSet 247
InstalledSoftwareSet 248
PortSet 250
ProcessSet 253
RegistryKeySet 256
RegistryValueSet 258
ServiceSet 260
UserSet 262
WQLSet 265
Multi-Node Manager 269
Options for Log Inspection Rules 272
Packet Processing Sequence 275
Ports Used by Deep Security 276
Protecting a Mobile Laptop 278
Recommendation Scans 287
Role-Based Access Control 289

© Copyright 2011 Trend Micro Inc.
All rights reserved.

System Events 295
Teamed NICs 307
Virtual Appliance 309

Known Issues.....313

Support 314

Legal Notice 315

Privacy Policy 316

© Copyright 2011 Trend Micro Inc.
All rights reserved.

How this document is organized

Deep Security 7.5 provides an introduction to Trend Micro's Deep Security 7.5 functionality and components.

What's new in Deep Security 7.5 is an overview of the major changes in this release.

The **Deep Security Manager Interface** section is a screen-by-screen description of the Deep Security Manager's user interface.

The **Deep Security Agent Interface** and **Deep Security Virtual Appliance Interface** sections describe the user interface details for the Deep Security Agent and Deep Security Virtual Appliance components.

The **How To...** section gives information on how to perform commonly used administrative tasks, and includes tips on configuration and best practices.

Reference is a technical reference guide that provides information on how rules work and how to program them, advanced configuration information, and where to find more information on known issues.

Support provides information on how to contact Trend Micro for customer support.

The remaining sections provide Trend Micro legal notices and information on the Privacy policy.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Deep Security 7.5

Deep Security 7.5 provides advanced protection for systems in the dynamic datacenter—from virtual desktops to physical, virtual or cloud servers. Deep Security provides comprehensive protection, including:

- Anti-Malware
- Intrusion Detection and Prevention (IDS/IPS) and Firewall
- Web Application Protection
- Application Control
- Integrity Monitoring
- Log Inspection

Deep Security consists of the following set of components that work together to provide protection:

- **Deep Security Manager**, the centralized management component which administrators use to configure security policy and deploy protection to enforcement components: Deep Security Virtual Appliance and Deep Security Agent.
- **Deep Security Virtual Appliance** is a security virtual machine built for VMware vSphere environments, that provides Anti-Malware, IDS/IPS, Firewall , Web Application Protection and Application Control protection.
- **Deep Security Agent** is a security agent deployed directly on a computer which can provide IDS/IPS, Firewall, Web Application Protection, Application Control, Integrity Monitoring and Log Inspection protection.

The following table identifies which protection is provided by the Deep Security Virtual Appliance, the Deep Security Agent, or both:

	Deep Security Agent	Deep Security Virtual Appliance
Anti-Malware	No	Yes
Firewall	Yes	Yes
Deep Packet Inspection	Yes	Yes
Integrity Monitoring	Yes	No
Log Inspection	Yes	No

Deep Security Manager

Deep Security Manager ("the Manager") is a powerful, centralized web-based management system that allows security administrators to create and manage comprehensive security policies and track threats and preventive actions taken in response to them. Deep Security Manager integrates with different aspects of the datacenter including: VMware vCenter, Microsoft Active Directory and has a web services API for integration with datacenter automation environments.

Security Profiles

Security Profiles are policy templates that specify the security rules to be configured and enforced automatically for one or more computers. These compact, manageable rule sets make it simple to provide comprehensive security without the need to manage thousands of rules. Default Security Profiles provide the necessary rules for a wide range of common computer configurations.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Dashboard

The customizable, web-based UI makes it easy to quickly navigate and drill down to specific information. It provides:

- Extensive system, event and computer reporting, with drill-down capabilities
- Graphs of key metrics with trends, with drill-down
- Detailed event logs, with drill-down
- Ability to save multiple personalized dashboard layouts

Built-in Security

Role-based access allows multiple administrators (Users), each with different sets of access and editing rights, to edit and monitor different aspects of the system and receive information appropriate to them. Digital signatures are used to authenticate system components and verify the integrity of rules. Session encryption protects the confidentiality of information exchanged between components.

Deep Security Agent and Deep Security Virtual Appliance

The Deep Security Agent ("the Agent") is a high performance, small footprint, software component that sits directly on a computer to provide protection. The Deep Security Virtual Appliance runs as a VMware virtual machine and protects the other virtual machines on the same ESX Server, each with its own individual security policy.

Anti-Malware Protection for VMware Virtual Machines

The Anti-Malware module features Trend Micro anti-malware protection, including virus remediation actions which clean, delete, deny access, or quarantine malicious software. Alerts can be generated when malicious software is detected. Deep Security integrates with VMware vShield Manager Endpoint Security to deliver anti-malware protection.

DPI Rules: Intrusion Detection and Prevention (IDS/IPS), Web Application Protection and Application Control

DPI Rules deliver Intrusion Detection and Prevention (IDS/IPS) protection by protecting vulnerabilities from known and unknown attacks. This type of protection is also known as virtual patching, and is achieved by each rule defining expected application data, and blocking malicious data based on its content.
In addition, DPI rules protect vulnerabilities such as Cross-Site Scripting (XSS) and SQL injection in web applications through a set of Web Application Protection rules.
DPI rules are also used to provide Application Control to computers, by detecting known application traffic that may need to be restricted in corporate environments.
Ongoing Deep Security Rule updates automatically provide the most current, comprehensive protection against known and unknown attacks.

Firewall Rules

A sophisticated, bi-directional stateful firewall provides complete support for all network protocols, including TCP, UDP and ICMP. Firewall Rules are fully configurable to allow or deny traffic on a per-interface basis, and restrict communication to allowed IP or MAC addresses.

Integrity Monitoring Rules

The Integrity Monitoring protection module allows the Deep Security Agents to scan for and detect changes to a computer system's files, directories, and registry keys and values, as well as changes in installed software and running services. These changes are logged as events in the Manager and can be configured to generate alerts.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Log Inspection Rules

With the integration of OSSEC, Deep Security has the ability to inspect the logs and events generated by the operating system and applications. Log Inspection events are saved in the Manager and can be configured to generate alerts.

System Requirements

Deep Security Manager

- **Memory:** 4GB
- **Disk Space:** 1.5GB (5GB recommended)
- **Operating System:** Microsoft Windows Server 2008 (32-bit, 64-bit), Windows Server 2008 R2 (64-bit), Windows 2003 Server SP2 (32-bit, 64-bit)
- **Database (Recommended but Optional):** Oracle 11g, Oracle 10g, Microsoft SQL Server 2008 SP1, Microsoft SQL Server 2005 SP2
- **Web Browser:** Mozilla Firefox 3.x (cookies enabled) , Internet Explorer 7.x (cookies enabled) , Internet Explorer 8.x (cookies enabled)

Deep Security Virtual Appliance

- **Memory:** 1GB
- **Disk Space:** 20GB
- **VMware Environment:**
  - VMware vCenter 4.1
  - ESXi 4.1
  - VMware Tools
  - VMware vShield Manager
  - VMware vShield Endpoint Security

For specifics about the VMware vShield environment please see the Installation Guide.

A virtualized ESX environment (ESX running as a VM) is not supported.

ESXi 4.1 Requirements for the Deep Security Virtual Appliance

In addition to the ESXi 4.1 standard system requirements, the following specifications must be met:

- **CPU:** 64-bit, Intel-VT present and enabled in BIOS
- **Supported vSwitch: standard vSwitch or 3rd party vSwitch – Cisco Nexus 1000v**

(When you create a new virtual machine, the default configuration does not include a SCSI controller. You must specifically add a SCSI controller to the virtual machine. For a list of supported LSI SCSI drivers and installation instructions, please consult your VMware Endpoint documentation.)

Deep Security Agent

- **Memory:** 128MB
- **Disk Space:** 100MB (200MB recommended, primarily for logging)
- **Supported Platforms:** Windows, Solaris, Linux, AIX, HP-UX

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Trend Micro endeavors to provide Deep Security Agents for new versions of each platform as they are released and may discontinue support for retired versions. Please see the Installation Guide and release notes for the currently supported versions of each platform.

The AIX and HP-UX Agents only support Integrity Monitoring and Log Inspection. For the latest information, consult the Install Guide and the Agent release notes.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

What's New in Deep Security 7.5

Anti-Malware for Virtual Machines

The Trend Micro Deep Security Virtual Appliance now supports Anti-Malware protection for virtual machines within VMware's vSphere 4.1 environment. The Deep Security Manager's new Anti-Malware module now supports:

- Protection of active virtual machines running on a ESXi 4.1
- Highly customizable Anti-Malware configurations applicable to security profiles and hosts
- Real-time, manual and scheduled scans
- Use of the Smart Protection Network
- Quarantined file management, including download and delete from DSM
- Anti-Malware support built in to Dashboard widgets and reports
- Anti-Malware Web service integration from the Deep Security Manager

Deep Security Virtual Appliance Protection Workflow Improvements

Improvements to the usability of the Deep Manager have made it simpler to get a Deep Security Virtual Appliance up a running in a VMware environment.

Performance and Scalability (DS 7.5 SP1)

Deep Security 7.5 SP1 brings increased overall performance and scalability by significantly improving the speed and efficiency of security update deployments, heartbeats, recommendation scans, memory usage, and the Deep Security Manager user interface.

Automatic Activation and/or Protection of Newly Added Computers (DS 7.5 SP1)

Alongside Scheduled Tasks, Event-based Tasks now let you automatically and conditionally activate and/or assign Security Profiles to computers that are:

- vMotioned onto a managed ESX host
- Created on a managed ESX host
- Added via Agent-initiated activation
- Added when an Active Directory is imported or synchronized

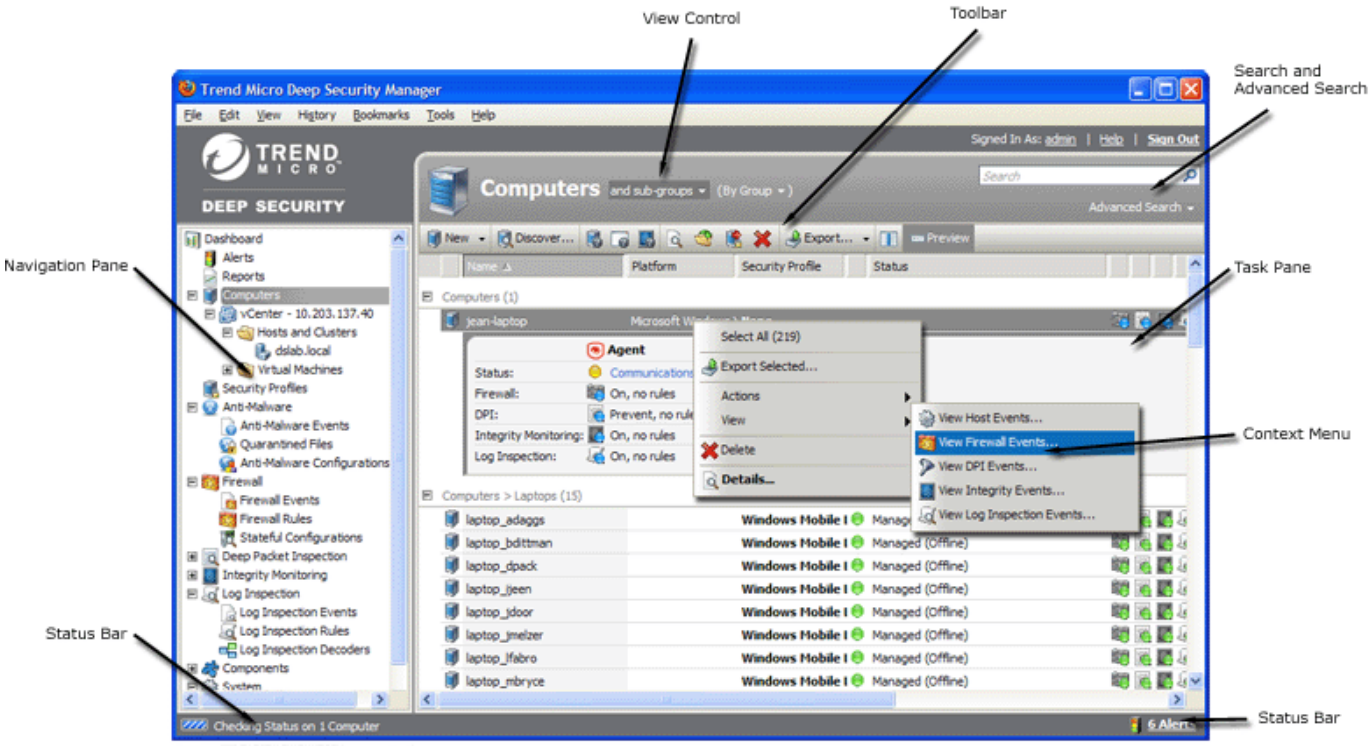
Multi-Language Support (DS 7.5 SP2)

Deep Security 7.5 is now available in multiple language versions. Please contact Trend Micro to find out what languages are available.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Deep Security Manager Interface

Deep Security Manager's web-based user interface was designed to provide you with easy access to all elements of the Deep Security system. The following are its main features.



Navigation Pane

The navigation pane contains the tree-based navigation system. Elements of the Deep Security system are organized as follows:

- **Dashboard:** an at-a-glance overview of the status of the Deep Security system
- **Alerts:** a summary of current critical and warning alerts concerning system or security events
- **Reports:** a report generator to produce summaries of system status and summaries of activities
- **Computers:** a list of computers discovered (or manually added) and managed on your network with status information for each
- **Security Profiles:** a list of defined Security Profiles
- **Anti-Malware**
  - **Anti-Malware Events:** logs of Anti-Malware activity
  - **Quarantined Files:** a list of files that have be been quarantined because they are suspected of being infected with malware
  - **Anti-Malware Configurations:** predefined Anti-Malware security settings that can be applied to new computers
- **Firewall**
  - **Firewall Events:** logs of security-related Firewall activity
  - **Firewall Rules:** where you define and manage Firewall Rules
  - **Stateful Configurations:** where you define and manage Stateful Configurations
- **Deep Packet Inspection**
  - **DPI Events:** logs of security-related DPI activity
  - **DPI Rules:** where you define and manage DPI Rules

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **Application Types:** Application Types are defined by connection direction, protocol, and ports. They define the traffic DPI Rules operate on.

- **Integrity**
  - **Integrity Monitoring Events:** logs of Integrity Monitoring activity
  - **Integrity Monitoring Rules:** the rules which scan for and detect changes to a computer's files, directories, and registry keys and value
- **Log Inspection:**
  - **Log Inspection Events:** The results of log inspection activity
  - **Log Inspection Rules:** OSSEC Rules which monitor and report on the logs and events generated by the computer's operating system
  - **Log Inspection Decoders:** required for the proper functioning of the Log Inspection Rules.
- **Components:** a list of common components used by various elements of the Deep Security system
- **System:** where you can find administrative tools to manage the operation of the Deep Security system, and view records and reports of system events

Task Pane

Clicking an element in the navigation pane will display that element's screen in the task pane. Almost all of your work will be done on a screen in the task pane. Where the task pane displays lists of items, columns can be added or removed by clicking the **Add/Remove Columns** button in the toolbar ( ). The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Pagination Controls

Some lists displayed in the task pane will contain more elements than can be shown on a single screen. When this is the case, the pagination information shows the subset of items you are viewing. Use the pagination tool to move from page to page of your list or enter an item number in the text box to start the list there. The number of items to display per page can be configured in the System section. (Pagination settings can be configured for each User by going to **System > Users > Properties > Settings > List Views**.)

View Control

Where appropriate, the view control gives you options for displaying listed items. For example, when you click a computer group in the navigation pane, computers belonging to that group will be listed in the task pane. The view control will let you choose between displaying only computers from that group, and displaying computers in that group and all sub-groups. Where appropriate, the view control lets you organize your listed items into categories. For example, you may want to group your listed computers by the Security Profile that has been assigned to them.

Whether or not Deep Security Manager remembers these settings if you navigate away from and return to a screen can be configured on the **Settings** tab in the Properties window for each individual User. (Go to **System > Users > Properties > Settings > List Views.**)

Toolbar

The toolbar holds buttons which carry out various actions specific to the screen you are working in. Most commonly, these will include buttons for the deletion, modification, and creation of list items. Many of the toolbar options are also available from the short-cut menu. The Deep Security Manager allows you to save your searches for reuse. This effectively lets you create reusable filters to apply to listed items.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Search and Advanced Search

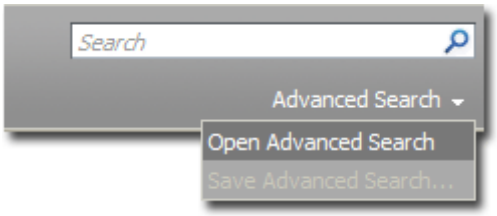
The simplest way to search is to use the "simple" search bar.

This will search the database for matches among the listed items (Firewall Events in the **Firewall** screen, System Events on the **System Events** screen, etc.)

Note that all items will be searched not just the ones currently displayed. For instance, if you are viewing Firewall Events for all computers over the last 7 days, the **Firewall Events** screen may display a message like "Only *the most recent 1,000 out of 55,056 items have been included. Consider using a narrower date range or additional search criteria.*" Even though only 1000 items are made available for display, all 55,056 items will be searched. The search engine will search through each field in the database except the date.

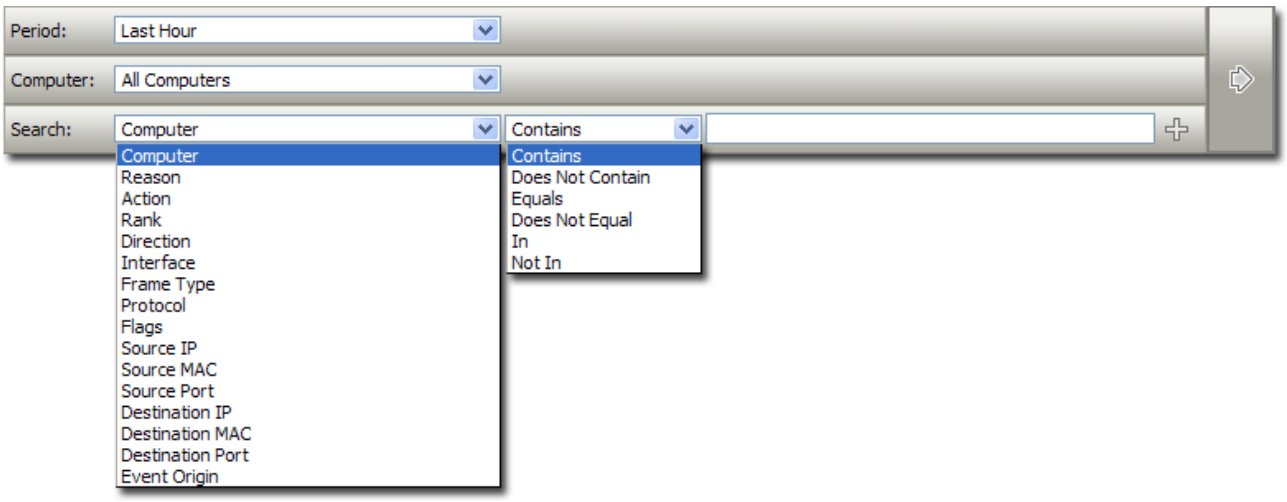
The number of items displayed can be configured in the **Properties** window for each individual User. (**System > Users**)

For more sophisticated searches, click "Advanced Search " and then "Open Advanced Search".



The **Period** toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The **Computers** toolbar lets you organize the display of event log entries by computer groups or computer Security Profiles.



© Copyright 2011 Trend Micro Inc.
All rights reserved.

Search functions (searches are not case sensitive):

- **Contains:** The entry in the selected column contains the search string
- **Does Not Contain:** The entry in the selected column does not contain the search string
- **Equals:** The entry in the selected column exactly matches the search string
- **Does Not Equal:** The entry in the selected column does not exactly match the search string
- **In:** The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In:** The entry in the selected column does not exactly match any of the comma-separated search string entries

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the toolbars with the right-arrow on it).

Whether or not Deep Security Manager remembers these settings if you navigate away from and return to a screen can be configured on the **Settings** tab in the Properties window for each individual User. (Go to **System > Users**)

Status Bar

The status bar displays information relating to the current state of your Deep Security system. The number of active alerts (if any) is displayed at the right edge of the status bar. The left side of the status bar dynamically displays what actions are currently in progress such as computer-discovery, port-scanning operations, Agent/Appliance activations, Agent/Appliance updates, or Agent/Appliance upgrades.

Shortcut Menus

Many of the Deep Security Manager's screens have context-sensitive menus. Right-clicking a security Profile, for example, gives you a shortcut menu with quick access to most of the options in the toolbar for that screen. Right-clicking a computer group displays a shortcut menu with options to manage the current group or create a new one.

Note that many elements of the UI display informative tool tips when the mouse pointer is held over them.

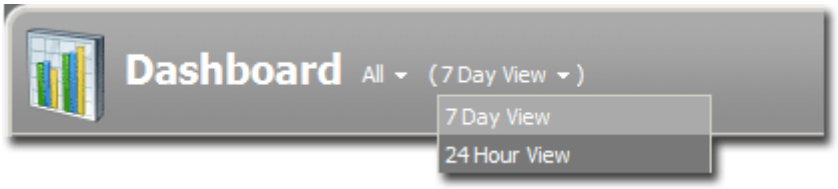
© Copyright 2011 Trend Micro Inc.
All rights reserved.

Dashboard

The Dashboard provides a quick at-a-glance view of the state of the Deep Security system. When logging in to the Deep Security Manager, the layout of the Dashboard is preserved from your last session. This applies to all Users who log in.

Date/Time Range

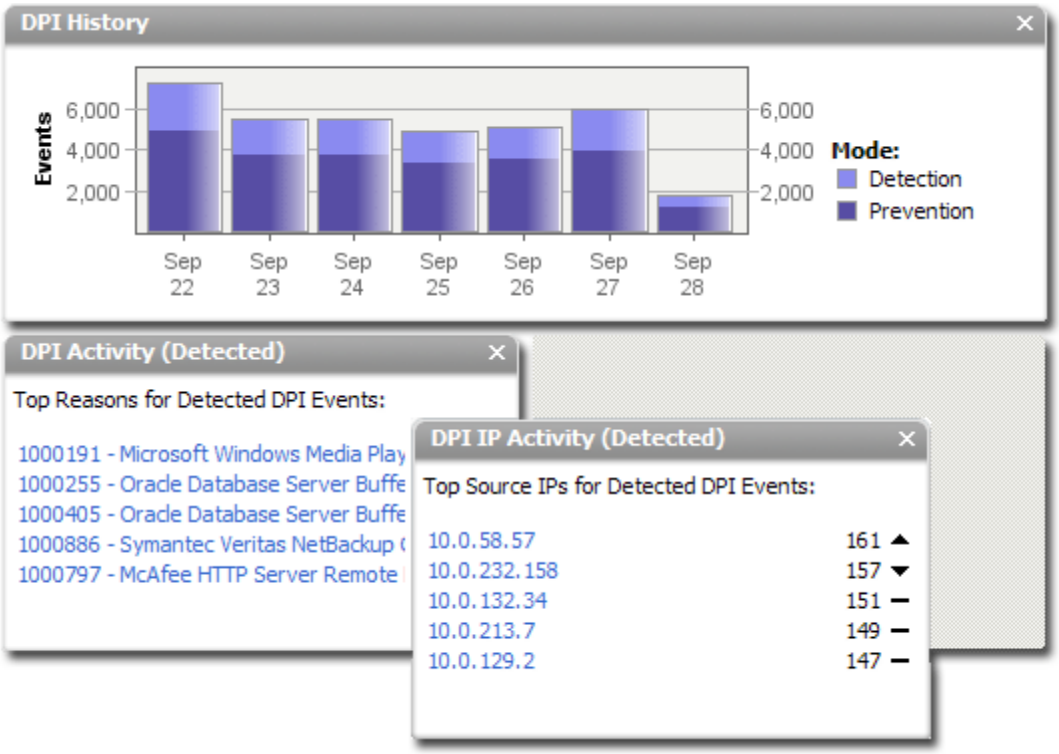
The Dashboard displays data from either the last 24 hours, or the last seven days. To switch between these two views, use the drop-down menu at the top of the screen.



"Widgets"

Information panels ("widgets") can be rearranged on the screen by dragging and dropping them to their new locations. Widgets can also be added to or removed from the Dashboard display.

© Copyright 2011 Trend Micro Inc.
All rights reserved.



Click **Add/Remove Widgets...** at the top right of the dashboard to view the list of available widgets.

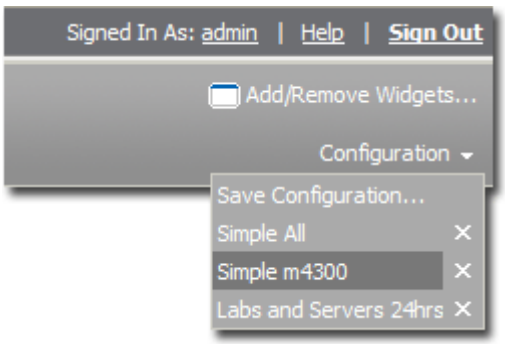
Many widgets contain links to let you "drill down" to the data. For example, clicking a column in the DPI History chart takes you to the **DPI Events** screen listing all the DPI Events that occurred on that day.

To remove a widget from the Dashboard, click the "X" in its top-right corner.

Note the trend indicators next to the numeric values in the 1x1 widgets. An upward or downward pointing triangle indicates an increase or decrease compared to the previous time period, and a flat line indicates no significant change.

Saving Dashboard Layouts

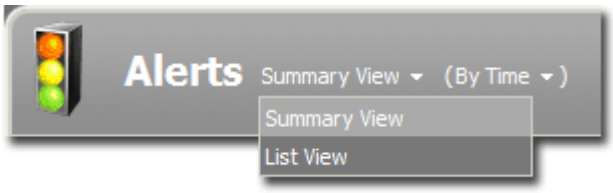
Individual Dashboard layouts can saved, loaded, and deleted using the **Configuration** menu at the top right of the dashboard.



© Copyright 2011 Trend Micro Inc.
All rights reserved.

Alerts

The **Alerts** screen displays all active alerts. Alerts can be displayed in a Summary View which will group similar alerts together, or in List View which lists all alerts individually. To switch between the two views, use the drop-down menu next to "Alerts" in the screen's title.



In Summary View, expanding an alert panel (by clicking **Show Details**) displays all the computers (and/or Users) that have generated that particular alert. (Clicking the computer will display the computer's **Details** window.)

In Summary View if the list of computers is longer than five, an ellipsis ("...") appears after the fifth computer. Clicking the ellipsis displays the full list. Once you have taken the appropriate action to deal with the alert, you can dismiss the alert by selecting the checkbox next to the target of the alert and clicking the **Dismiss** link. (In List View, right-click the alert to see the list of options in the context menu.)

Alerts can be of two types: system and security. System alerts are triggered by System Events (Agent Offline, Clock Change on Computer, etc.) Security alerts are triggered by DPI, Firewall, Integrity, and Log Inspection Rules. Alerts can be configured by clicking **Configure Alerts...**.

Use the computers filtering bar to view only alerts for computers in a particular computer group, with a particular Security Profile, etc.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Reports

Deep Security Manager produces reports in PDF, or RTF formats. Most of the reports generated by the **Reports** screen have configurable parameters such as date range or reporting by computer group. Parameter options will be disabled for reports to which they don't apply.

Report

The various reports can be output to PDF or RTF format.

Tag Filter

When you select a report which contains event data, you have the option to filter the report data using Event Tags. Select **All** for only tagged events, **Untagged** for only untagged events, or select **Tag(s)** and specify one or more tags to include only those events with your selected tag(s).

Time Filter

You can set the time filter for any period for which records exist. This is useful for security audits.

Reports use data stored in counters. Counters are data aggregated periodically from Events. Counter data is aggregated on an hourly basis for the most recent three days. Data older than three days is stored in counters that are aggregated on a daily basis. For this reason, the time period covered by reports for the last three days can be specified at an hourly level of granularity, but beyond three days, the time period can only be specified on a daily level of granularity.

Computer Filter

Set the computers whose data will be included in the report.

Encryption

Reports can be protected with the password of the currently signed in User or with a new password for this report only.

Tip: To generate a report on specific computers from multiple computer groups, create a User who has viewing rights only to the computers in question and then either create a Scheduled Task to regularly generate an "All Computers" report for that User or log in as that User and run an "All Computers" report. Only the computers to which that User has viewing rights will be included in the report.

If your reporting requirements are not met by the original reports included with Deep Security Manager, it may be possible to have custom reports designed for you. Please contact your support provider for more information.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Computers

The **Computers** screen allows you to manage and monitor the computers on your network. This screen updates itself periodically. The time between updates can be set from your User **Properties** window on the **Settings** tab (**System > Users**).

Computer icons:

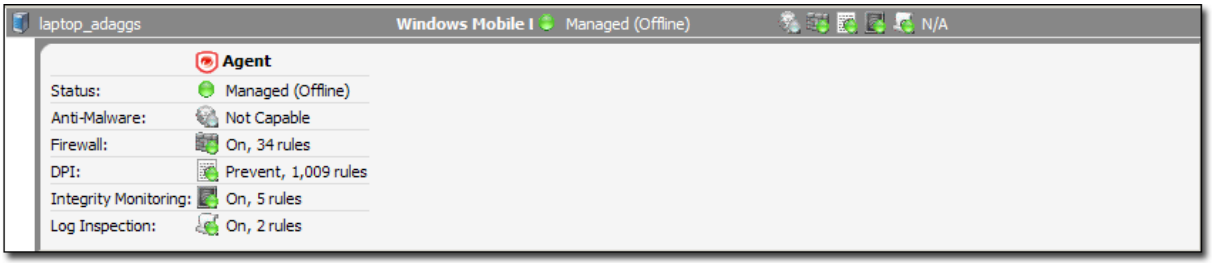
- Ordinary computer
- ESX Server
- Virtual computer
- Virtual computer (started)
- Virtual computer (stopped)
- Virtual computer (suspended)
- Virtual Appliance
- Virtual Appliance (started)
- Virtual Appliance (stopped)
- Virtual Appliance (suspended)

Preview Pane

Clicking on **Preview** in the toolbar expands a display area beneath a listed computer.

Ordinary Computer

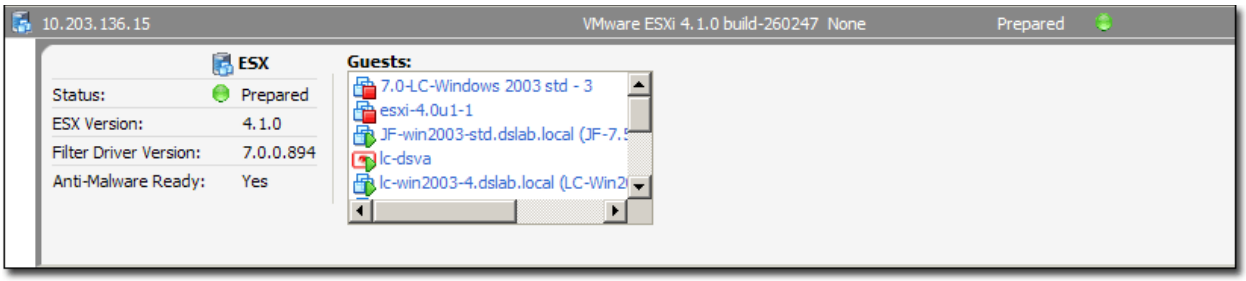
The preview pane for an ordinary computer displays the presence of an Agent, its status, and details about the Firewall, DPI, Integrity Monitoring, and Log Inspection modules.



ESX Server

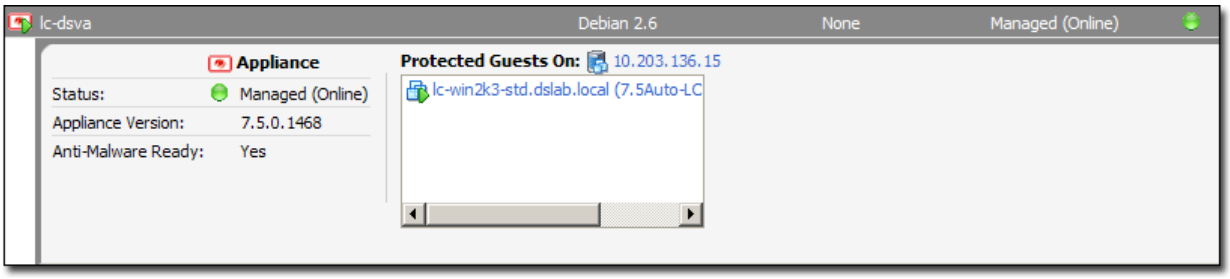
The preview pane for an ESX Server displays its status, the version numbers of the ESX software and the Deep Security Filter Driver. In the **Guests** area are displayed the presence of a Deep Security Virtual Appliance, and the virtual machines running on this host.

© Copyright 2011 Trend Micro Inc.
All rights reserved.



Virtual Appliance

The preview pane for a Virtual Appliance whether it is being managed by the Deep Security Manager, and which virtual machines are being protected.



Virtual Machine

The preview pane for a virtual machine displays whether it is being protected by a Virtual Appliance, an in-guest Agent, or both. It displays details about the components running on the virtual machine. Since the Appliance is not capable of providing Integrity Monitoring or Log Inspection protection at this time, they will appear as "Not Capable". Firewall and DPI configuration will always be the same for both the Appliance and the in-guest Agent.

Remember that a virtual machine can run an Agent as though it were an ordinary computer managed by the Deep Security Manager. It does not need to be "imported" into the Manager by way of a vCenter integration. For more information on VMware integration, see the Installation Guide.

Adding Computers

For more detailed instructions on adding computers to the Deep Security Manager see the *Getting Started* section or *Add Computers to the Manager* in the **How To...** section.

After being installed on a computer, an Agent must be "activated" by the Deep Security Manager. During this process, the Deep Security Manager sends a "fingerprint" to the Agent. From that point on, the Agent will only accept instructions from a Manager with that unique fingerprint.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

If you install an Agent on a virtual machine that was previously being protected Agentlessly by a Deep Security Virtual Appliance, the virtual machine will have to be activated again from the Manager to register the presence of the Agent on the computer.

Define a New Computer

Clicking **New** in the toolbar displays a computer creation wizard. Type the hostname or IP address of the new computer and optionally select a Security Profile to be applied to the new computer from the drop-down list. Clicking **Next** will tell the Manager to find the computer on the network.

- **If the computer you specified is not found,** the Manager will still create an entry for it in the **Computers** screen, but you will have to ensure that the Manager can reach this computer and that the Agent is installed and activated. Then you can apply the appropriate Security Profile to it.
- **If the computer is found but no Agent is identified,** the Manager will create an entry for the computer on the **Computers** screen. You will have to install an Agent on the computer and activate it.
- **If the computer is found and an Agent is detected,** the Manager will create an entry in the **Computers** screen. As soon as you exit the wizard (by clicking **Finish**), the Manager will activate the Agent on the computer and apply the Security Profile you selected.

Discover Computers

Clicking **Discover...** in the toolbar displays the **Discover Computers** dialog. During discovery, the Manager searches the network for any visible computers that are not already listed. When a new computer is found, the Manager attempts to detect whether an Agent is present. When discovery is complete, the Manager displays all the computers it has detected and displays their status in the **Status** column. After discovery operations, a computer can be in one of the following states:

- **Discovered (No Agent/Appliance):** The computer has been detected but no Agent/Appliance is present. The computer may also be in this state if an Agent/Appliance is installed but has been previously activated and is configured for Agent/Appliance initiated communications. In this case, you will have to deactivate the Agent/Appliance on the computer and reactivate it from the Manager.
- **Discovered (Activation Required):** The Agent is installed and listening for communication from the Manager, but has not been activated. This status may also indicate that the Agent/Appliance is installed and listening, and has been activated, but is not yet being managed by the Manager. This could occur if this Manager was at one point managing the Agent/Appliance, but the Agent/Appliance's public certificate is no longer in the Manager's database. This may be the case if the if the computer was removed from the Manager and then discovered again. To begin managing the Agent/Appliance on this computer, right-click the computer and select "Activate/Reactivate". Once reactivated, the status will change to "Online".
- **Discovered (Deactivation Required):** The Agent/Appliance is installed and listening, but it has already been activated by another Manager. In this case the Agent/Appliance must be deactivated prior to activation by this Manager.

The Discovery operation will only check the status of newly discovered computers. To update the status of already listed computers, right-click the selected computer(s) and select **Actions > Update Now**.

When discovering computers you can specify a computer group to which they should be added. Depending on how you have chosen to organize your computer groups, it may be convenient to create a computer group called "Newly Discovered Computers", or "Newly Discovered Computers on Network Segment X" if you will be scanning multiple network segments. You can then move your discovered computers to other computer groups based on their properties and activate them.

When running a Discovery operation with the **Automatically Resolve IPs to hostnames** option enabled, it is possible that the discovery operation will find hostnames where Deep Security Manager can not. Discovery is able to fall back to using a WINS query or NetBIOS broadcast to resolve the hostname in addition to DNS. Deep Security Manager only supports hostname lookup via DNS.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

The Discovery operation will not discover computers running as virtual machines in a vCenter or computers in a Directory/Active directory.

Add Directory

Deep Security Manager can connect to and synchronize with a Microsoft Active Directory. For detailed instructions on importing a list of computers from an Active Directory, see the *Add Computers to the Manager* in the **How To...** section.

Add VMware vCenter

Deep Security Manager supports a tight integration with VMware vCenter and ESX Server. You can import the organizational and operational information from vCenter and ESX nodes and allow detailed application of security to an enterprise's VMware infrastructure. For detailed instructions on importing virtual computers from a VMware system, see the Installation Guide .

Scan Computers for Open Ports

Scan for Open Ports performs a port scan on all selected computers and checks the Agent installed on the computer to determine whether its state is either "Deactivation Required", "Activation Required", "Agent Reactivate Required", or "Online". (The scan operation, by default, scans ports 1-1024. This range can be changed in the **System > System Settings** section under the **Scan** tab.)

Port 4118 is always scanned regardless of port range settings. It is the port on the computer to which Manager initiated communications are sent. If communication direction is set to "Agent/Appliance Initiated" for a computer (**Computer Details > System > System Settings > Computer > Communication Direction**), port 4118 is closed.

New computers on the network will not be detected. To find new computers you must use the **Discover** tool.

Scan for Recommendations

Deep Security Manager can scan computers and then make recommendations for Security Rules. The results of a recommendation scan can be seen in the computer's **Details** window in the various **Rules** screens. See the documentation for the **Computer Details** screen for more information.

Recommendation Scans can only be performed on computers on which a Deep Security Agent is installed. This function is not available on computers protected only by a Virtual Appliance.

Scan for Integrity Changes

Integrity Monitoring tracks changes to a computer's system and files. It does by creating a baseline and then performing periodic scans to compare the current state of the computer to the baseline. For more information see the documentation for the **Integrity Monitoring** screen.

Move a Computer to a Computer Group

To move a computer to new computer group, right-click the computer and choose **Actions > Move to Group...**

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Assign a Security Profile to a Computer

This opens a window with a drop-down list allowing you to assign a Security Profile to the computer. The name of the Security Profile assigned to the computer will appear in the **Security Profile** column on the **Computers** screen.

Note that if you apply other settings to a computer (for example, adding additional Firewall Rules, or modifying stateful configuration settings), the name of the Security Profile will be in bold indicating that the default settings have been changed.

Assign an Asset Value

Asset values allow you to sort computers and events by importance. The various Security Rules have a severity value. When a rules are triggered on a computer, the severity values of the rules are multiplied by the asset value of the computer. This value is used to rank events in order of importance. For more information see **System > System Settings > Ranking**.

Delete a Computer

If you delete a computer, all information pertaining to that computer is deleted along with it. If you re-discover the computer, you will have to re-assign a Security Profile and whatever rules were assigned previously.

Search for a Computer

Use the **Search** textbox to search for a particular computer among already discovered (i.e. listed) computers. (To find a computer on the network that is not yet listed, use New ( ).) For more sophisticated search options, use the "Advanced Search" option below it.

Advanced Search functions (searches are not case sensitive):

- **Contains:** The entry in the selected column contains the search string
- **Does Not Contain:** The entry in the selected column does not contain the search string
- **Equals:** The entry in the selected column exactly matches the search string
- **Does Not Equal:** The entry in the selected column does not exactly match the search string
- **In:** The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In:** The entry in the selected column does not exactly match any of the comma-separated search string entries

Export Selected Computers

Export your computers data to an XML file. You may wish to do this to backup your computer information, integrate it with other reporting systems, or if you are migrating computers to another Deep Security Manager. (This will save you the trouble of re-discovering and scanning computers from the new Manager.)

Note that the exported computers file does **not** include any assigned Security Profiles, Firewall Rules, Stateful Configurations or DPI Rules. In order to export this configuration information use the Security Profile export option in the **Security Profiles** screen.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Activate/Reactivate the Agent/Appliance on a Computer

When a computer is unmanaged the Agent/Appliance must be activated to move the computer into a managed state. Prior to activation the Agent/Appliance will be one of the following states: On the **Computers** screen, right-click the computer whose Agent/Appliance you wish to Activate/Reactivate and select "Activate/Reactivate" from the **Actions** menu. (Alternatively, you can click the **Activate** or **Reactivate** button in the computer's **Details** window.)

- **No Agent/Appliance:** Indicates there is no Agent/Appliance running or listening on the default port. The "No Agent/Appliance" status can also mean that an Agent/Appliance is installed and running but is working with another Manager and communications are configured as "Agent/Appliance Initiated", and so the Agent/Appliance is not listening for this Manager. (If you wish to correct the latter situation, you will have to deactivate the Agent from the computer).
- **Activation Required:** The Agent/Appliance is installed and listening, and is ready to be activated by the Manager.
- **Reactivation Required:** The Agent/Appliance is installed and listening and is waiting to be reactivated by the Manager.
- **Deactivation Required:** The Agent/Appliance is installed and listening, but has already been activated by another Manager.
- **Unknown:** The computer has been imported (as part of an imported computer list) without state information, or has been added by way of an LDAP directory discovery process.

After a successful activation the Agent/Appliance state will change to "Online". If the activation failed the computer status will display "Activation Failed" with the reason for the failure in brackets. Click this link to display the system event for more details on the reason for the activation failure.

Check the Status of a Computer

This command simply checks the status of a computer without performing a scan or activation attempt.

Deactivate the Agent/Appliance on a Computer

You may want to transfer control of a computer from one Deep Security Manager installation to another. If so, the Agent has to be deactivated and then activated again by the new Manager. Deactivating the Agent can be done from the Manager currently managing the Agent. *Deactivating an Agent may also be done directly on the computer from the command line. Deactivating an Appliance may also be done directly on the ESX Server console by selecting Reset Appliance*

Update the Agent on a Computer

Updating the Agent on a computer deploys any configuration changes you have made for that computer from the Manager to the Agent. Updates occur automatically at every heartbeat, but if you wish to apply your changes immediately, you can use this option. The **Update Now** button can be used to override the computer access schedule or to force the Manager to retry an update if the previous attempt failed.

Note that the automatic updates actually occur immediately if the communications are not Agent/Appliance initiated, and they occur on the next heartbeat if Agent/Appliance initiated.

Get Events from Computer(s)

Override the normal event retrieval schedule (usually every heartbeat) and retrieve the Event logs from the computer(s) now.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Clear Warnings/Errors

This command will clear any warnings or errors generated for a computer whose Agent has been reset locally or has simply been removed from the network before a User has had a chance to deactivate or delete the computer from the list of computers.

Lock an Agent

You can lock a computer if you are going to perform some maintenance on it and don't want to trigger a series of alerts on the Manager.

The computer's status will be displayed as "locked" while in this state and the Manager will not communicate with the Agent or trigger any computer/Agent related alerts. Existing computer alerts are not affected. If an update is in progress it will be allowed to complete normally.

Note that the Agent is not told that the computer is in a locked state. If communication between the Agent and the Manager has been set to "Agent/Appliance Initiated" or "Bi-directional", it may generate an event which it will report when it finally contacts the Manager again.

Unlock an Agent

Unlock a locked Computer. (See above.)

Upgrade the Agent Software on a Computer

To upgrade an Agent you first need to add an authenticated **Agent Install** program to the Deep Security Manager.

1. Go to the **Software** section in the **System > Updates** screen and click the **View Software** button. This will display the **Software** screen. Click **New** to display the **Import Software** wizard.
2. If you don't already have an **Install** program locally, click the download link to see if any upgrades are available.
3. Select the install program (.msi, .rpm, or .zip) and click **Next**.
4. If you are uploading the software from a remote computer this may take a couple of seconds (Firefox displays a message in its status bar ("sending request to computer") but IE displays nothing.)
5. If the install program does not appear to be in the correct format an error message will appear at the top of the screen.
6. When you have successfully loaded the Agent software file you will get a confirmation window that lists the file name, the platform to which the installer applies, the version of the Agent program, a SHA-1 fingerprint of the program and a User-editable field for any custom notes you may want to apply.

Once an install program has been imported you can use it to upgrade one or more Agents.

1. On the **Computers** screen, right-click the computers whose Agents you wish to upgrade and select "Upgrade Agent software". (Alternatively, you can click the **Upgrade Agent** button in the computer's **Details** window.)
2. If there are no installers of an appropriate platform and version (the version must be higher than the Agent's) the following message will be displayed: "There are no authenticated Agent Software Install Programs available for the selected computer(s) platform or version. Please add an appropriate Agent Software Install Program using the **Software** panel in the **System > Updates** screen before upgrading the Deep Security Agents." Otherwise a dialog appears allowing you to select a specific version (or simply the latest version for the platform) and an upgrade schedule (or the default "use computer access schedule.")

© Copyright 2011 Trend Micro Inc.
All rights reserved.

In rare circumstances the computer may require a reboot to complete the upgrade. If this is the case, an Alert will be triggered. To find out right away whether a reboot is required, check the text of the "Agent Software Upgraded" event to see if the platform installer indicated that a reboot is required.

The "Reboot Required" Alert must be dismissed manually, it will not be dismissed automatically.

Cancel any Currently Executing Port Scans

If you have initiated a set of port scans to a large number of computers and/or over a large range of ports and the scan is taking too long, use this option to cancel the scans.

Clear Recommendations

Clear Rule recommendations resulting from a Recommendation Scan on this computer. This will also remove the computer from those listed in an Alert produced as a result of a Recommendation Scan.

Note that this action will not un-assign any rules that were assigned because of past recommendations.

Assign Computer Asset Value

A computer Asset Value is a (customizable) rating system used to assign value to computers. Each grade in the rating system has a value between 1 and 100. This value gets multiplied by the severity value of a rule to allow you to rank Firewall and DPI Rule Events. To configure Ranking, go to **System > System Settings > Ranking**.

Examine Events Associated with a Computer

Examine system and administrative events (that is, non security-related events) associated with a particular computer.

Examine a Computer's Event Logs

Examine the latest event logs uploaded from the Agent on this computer.

Add a New Computer Group

Creating computer groups is useful from an organizational point of view and it speeds up the process of applying and managing Security Profiles. Right-click the computer group under which you want to create the new computer group and select **Add Group**.

Add Computers and Computer Groups Imported from a Microsoft Active Directory structure

Discover computers by importing from an LDAP-based directory (such as Microsoft Active Directory). Computers are imported, and synchronized according to the structure in the directory. For more information, see Adding Computers to the Manager.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Remove a Group

You can only remove a computer group if it contains no computers and has no sub-groups.

Move Computers from the Current Group to Another

You can move a computer from one computer group to another but keep in mind that Security Profiles are applied at the computer level, not the computer group level. Moving a computer from one computer group to another has no effect on the Security Profile assigned to that computer.

View or Edit the Properties of a Computer Group

The properties of groups include their name and description.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Computer Details

The computer's **Details** window mirrors the main interface of the Deep Security Manager. It includes all the settings and configurations that can be changed to override any higher level settings and configurations.

Computer Information Screen

General

- **Hostname:** Appears in the **Name** column on the **Computers** screen. The name must be either the IP address of the computer or the hostname of the computer. (Either a fully qualified hostname or a relative hostname may be used if a hostname is used instead of an IP address.)
- **Display Name:** Appears in the Display Name column and in brackets next to the Hostname value.
- **Description:** a description of the computer.
- **Platform:** Details of the computer's OS will appear here.
- **Group:** The computer group to which the computer belongs appears in the drop-down list. You can reassign the computer to any other existing computer group.
- **Security Profile:** The Security Profile (if any) that has been assigned to this computer.

Keep in mind that if you unassign a Security Profile from a computer, Rules may still be in effect on the computer if they were assigned independently of the Security Profile.

- **Asset Importance:** Deep Security Manager uses a ranking system to quantify the importance of Security Events. Rules are assigned a Severity Level (high, medium, low, etc.), and Assets (computers) are assigned an "Asset Importance" level. These levels have numerical values. When a Rule is triggered on a computer the Asset Importance value and the Severity Level value are multiplied together. This produces a score which is used to sort Events by importance. (Event ranking can be seen in the **Events** screens.) Use this **Asset Importance** drop-down list to assign an Asset Importance level to this computer. (To edit the numerical values associated with severity and importance levels, go to **System > System Settings > Ranking**.)
- **Lock Computer (Prevents all communication):** Setting this option blocks all communications between the Agent/Appliance and the Manager. The computer's Security Profile is still active (all rules are still applied to all traffic), but should any alerts be generated, they will not be sent to the Manager.

You may wish to lock out a computer if you are going to perform some maintenance on it and don't want a series of alerts to appear in the Manager.

Status

- **Status:**
  - When the computer is unmanaged the status represents the state of the Agent/Appliance with respect to activation. The status will display either "Discovered" or "New" followed by the Agent/Appliance state in brackets ("No Agent/Appliance", "Unknown", "Reactivation Required", "Activation Required", or "Deactivation Required").
  - When the computer is managed and no computer errors are present, the status will display "Managed" followed by the state of the Agent/Appliance in brackets ("Online" or "Offline").
  - When the computer is managed and the Agent/Appliance is in the process of performing an action (e.g., "Integrity Scan in Progress", "Upgrading Agent(Install Program Sent)", etc.) the task status will be displayed.
  - When there are errors on the computer (e.g., "Offline", "Update Failed", etc.) the status will display the error. When more than one error is present, the status will display "Multiple Errors" and each error will be listed beneath.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **Anti-Malware:**
  - When Anti-Malware protection is on and either Real-Time or Scheduled scanning is in effect, Anti-Malware status will be "On" and the Anti-Malware status light will be green.
  - When Anti-Malware protection is on but neither Real-Time nor Scheduled scanning is in effect, Anti-Malware status will be "On" and the Anti-Malware status light will be blue.
  - When Anti-Malware protection is off and either Real-Time or Scheduled scanning is in effect, Anti-Malware status will be "Off" and the Anti-Malware status light will be blue.
  - When Anti-Malware protection is off and neither Real-Time nor Scheduled scanning is in effect, Anti-Malware status will be "Off" and the Anti-Malware status light will be blue.
- **Firewall:** Whether the Firewall is on or off and how many rules are in effect.
- **DPI:** Whether DPI is on or off and how many rules are in effect.
- **Integrity Monitoring:** Whether Integrity Monitoring is on or off and how many rules are in effect (Agent only).
- **Log Inspection:** Whether Log Inspection is on or off and how many rules are in effect (Agent only).
- **Online:** Indicates whether the Manager can currently communicate with the Agent/Appliance.
- **Last Communication:** The last time the Manager successfully communicated with the Agent/Appliance on this computer.
- **Check Status:** This button allows you to force the Manager to perform an immediate heartbeat operation to check the status of the Agent/Appliance. Check Status will not perform an update of the Agent/Appliance. (If an update is required click the **Update Now** button on the **Actions** tab.) When Manager to Agent/Appliance Communications is set to "Agent/Appliance Initiated" the **Check Status** button is disabled. (Checking status will not update the logs for this computer. To update the logs for this computer, go to the **Actions** tab.)
- **Clear Warnings/Errors:** Dismisses any alerts or errors on this computer.
- **ESX Server:** If the computer is a virtual machine protected by a Virtual Appliance, the hosting ESX Server is displayed.
- **Appliance:** If the computer is a virtual machine protected by a Virtual Appliance, the protecting Appliance is displayed.
- **ESX Version:** If the computer is an ESX Server, the ESX version number is displayed.
- **Filter Driver version:** If the computer is an ESX Server, the Filter Driver version number is displayed.
- **Guests:** If the computer is an ESX Server, the Virtual Appliance and Guests are displayed.
- **Appliance Version:** If the computer is a Virtual Appliance, the Appliance version number is displayed.
- **Anti-Malware Ready:** If the computer is a virtual machine, Anti-Malware Ready indicates whether or not the VMware VShield Endpoint Thin Client has been installed. If the computer is a Virtual Appliance, Anti-Malware Ready indicates whether or not the VMware VShield Endpoint driver has been installed on the hosting ESXi server.
- **Protected Guests On:** If the computer is a Virtual Appliance, the IP of the ESX Server and the protected Guest are displayed.

VMware Virtual Machine Summary

This section displays a summary of hardware and software configuration information about the virtual machine on which the Agent/Appliance is running (VMware virtual machines only).

Activation

A newly installed Deep Security Agent/Appliance needs to be "activated" by the Deep Security Manager before Security Profiles, Rules, requests for Event logs, etc. can be sent to it. The activation procedure includes the exchange of SSL keys which uniquely identify a Manager (or one of its nodes) and an Agent/Appliance to each other. Once activated by a Deep Security Manager, an Agent/Appliance will only accept instructions or communicate with the Deep Security Manager which activated it (or one of its nodes).

An unactivated Agent/Appliance can be activated by any Deep Security Manager.

Agents/Appliances can only be deactivated locally on the computer or from the Deep Security Manager which activated it. If an Agent/Appliance is already activated, the button in this area will read "Reactivate"

© Copyright 2011 Trend Micro Inc.
All rights reserved.

rather than "Activate". Reactivation has the same effect as Activation. A reactivation will reset the Agent/Appliance to the state it was in after first being installed and initiate the exchange of a new set of SSL keys.

Update

When you change the configuration of an Agent/Appliance on a computer using the Deep Security Manager (Apply a new DPI Rule, change logging settings, etc.) the Deep Security Manager has to send the new information to the Agent/Appliance. This is an update. Updates usually happen immediately but you can force an update by clicking the "Update Now" button.

Software

This displays the version of the Agent/Appliance currently running on the computer. If a newer version of the Agent/Appliance is available for the computer's platform you can click the "Upgrade Agent..." or "Upgrade Appliance..." button to remotely upgrade the Agent or Appliance from the Deep Security Manager. You can configure the Deep Security Manager to trigger an alert if new Agent/Appliance versions for any of your computers by going to **System > Updates** in the main Deep Security Manager window.

Support

The **Create Diagnostic Package...** button creates a snapshot of the state of the Agent/Appliance on the computer. Your support provider may request this for troubleshooting purposes.

If you have lost communication with the Computer, a diagnostics package can be created locally.

To create a diagnostics package locally on a Windows computer:

1. From a command line, type:
   ```
   C:\Program Files\Trend Micro\Deep Security Agent> dsa_control.exe /d
   ```
   and press **Enter**.
2. A numbered zip file (for example, "341234567.zip") containing the diagnostics information will be created in the same directory.

To create a diagnostics package locally on a Linux computer:

1. From a command line, type:
   ```
   $ /opt/ds_agent/dsa_control -d
   ```
   and press **Enter**.
2. A numbered zip file (for example, "341234567.zip") containing the diagnostics information will be created in the same directory.

To create a diagnostics package locally on a Deep Security Virtual Appliance computer:

1. 1.From a command line, type:
   ```
   $ sudo /opt/ds_agent/dsa_control -d
   ```
   and press **Enter**.
2. A numbered zip file (for example, "341234567.zip") containing the diagnostics information will be created in the same directory.

Interfaces

Displays the interfaces detected on the computer. If a Security Profile with multiple interface assignments has been assigned to this computer, interfaces that match the patterns defined in the Security Profile will be identified.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Alerts

Alerts are displayed the same way as they are in the main Deep Security Manager window except that only alerts relating to this computer are displayed. When an Alert is dismissed here, it is also dismissed in the main Deep Security Manager window.

Anti-Malware

Anti-Malware

You can set the Computer to inherit the Anti-Malware On/Off configuration from the global or Security Profile levels or you can uncheck **Inherit** and set the status independently.

Anti-Malware Scan

This area lists the last time manual and scheduled scan were run on this computer.

Click the **Scan for Malware** button to initiate a manual Anti-Malware scan, and click the **Abort Malware Scan** to stop it.

Remember that Manual, Scheduled, and Real-Time scans can have different properties. For a list of available Anti-Malware Configurations, see **Anti-Malware > Anti-Malware Configurations** in the main Deep Security Manager window. To see how the available Anti-Malware Configurations have been implemented for Manual, Scheduled, and Real-Time scans on this computer, see the **Anti-Malware > Anti-Malware Configurations** screen for the Security Profile assigned to this computer and the **Anti-Malware > Anti-Malware Configurations** screen of this computer itself.

Component Version

Displays which versions of the Anti-Malware components are installed on this Computer.

If this computer is an activated Virtual Appliance, you can click the **Update Anti-Malware Components...** button to install the latest versions of the components that are stored at the Deep Security Manager.

Note that the Virtual Appliance will be updated with the latest components from the Deep Security Manager, which may not be the latest versions available from Trend Micro. To make sure the Deep Security Manager has the latest components available from Trend Micro, in the Deep Security Manager main window, go to **System > Updates** and click **Update Now...** in the **Update Components** area.

Firewall (Firewall Rules, Stateful Configurations)

The Firewall for this computer inherits its on or off state either from its Security Profile or the global setting in the Deep Security Manager unless you choose to override it.

Note that if a Security Profile with Firewall turned off is applied to a computer and that computer is set to inherit firewall settings, all Firewall elements (Firewall Rules and Stateful Configurations) will be turned off on that computer, even elements that were assigned directly to the computer before the Security Profile was applied.

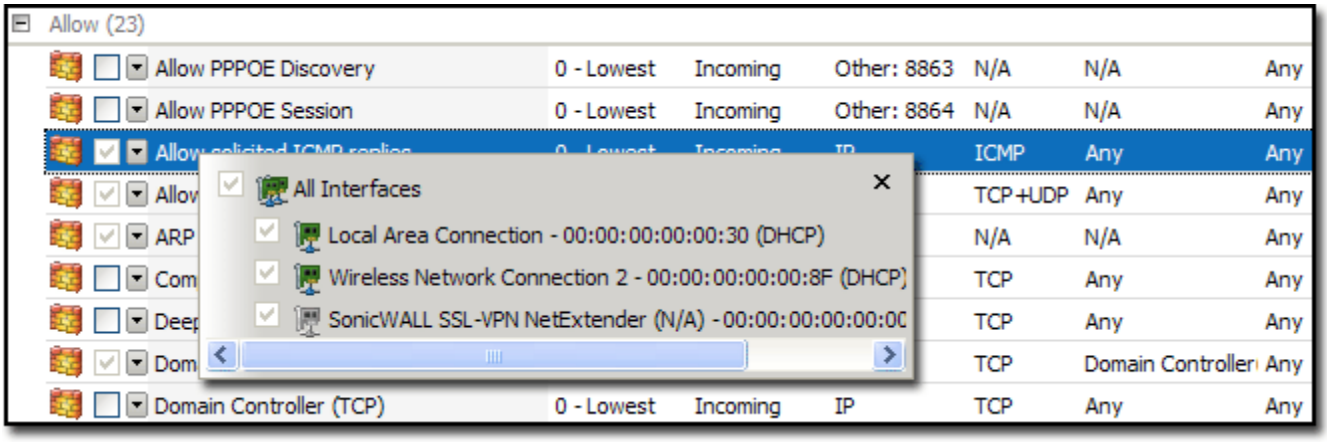
© Copyright 2011 Trend Micro Inc.
All rights reserved.

Events

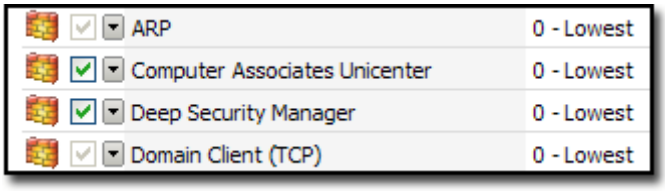
Firewall Events are displayed the same way as they are in the main Deep Security Manager window except that only events relating this computer are displayed.

Rules

The Firewall Rules defined in the Deep Security Manager are displayed here. Select which ones will be active on this computer. If the computer has multiple interfaces, click the down-arrow and use the drop-down menu to select whether the Firewall Rule will apply to all interfaces or to specific interfaces only.


Allow (23)
Allow PPPOE Discovery 0 - Lowest Incoming Other: 8863 N/A N/A Any
Allow PPPOE Session 0 - Lowest Incoming Other: 8864 N/A N/A Any
ICMP Any Any
TCP+UDP Any Any
N/A N/A Any
TCP Any Any
TCP Any Any
TCP Domain Controller Any
Domain Controller (TCP) 0 - Lowest Incoming IP TCP Any Any
All Interfaces
Local Area Connection - 00:00:00:00:00:30 (DHCP)
Wireless Network Connection 2 - 00:00:00:00:00:8F (DHCP)
SonicWALL SSL-VPN NetExtender (N/A) - 00:00:00:00:00:0C

Note the checkmarks next to the active firewall rules. Grayed-out checkmarks indicate that the Firewall Rule is active on this computer because it has been applied by a Security Profile. (The same applies to any other type of rule.)



Stateful Configurations

Select which Stateful Configuration to apply to this computer (if any). If the computer has multiple interfaces you can specify independent configurations for each interface.

Deep Packet Inspection (Events, Rules, Application Types)

The DPI engine for this computer inherits its on or off state, its Inline behavior, and it Recommendation Scan behavior from the global setting in the Deep Security Manager or the Security Profile assigned to it unless you choose to override it.

Events

DPI Events are displayed the same way as they are in the main Deep Security Manager window except that only events relating to this computer are displayed.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Rules

The DPI Rules defined in the Deep Security Manager are displayed here. Select which ones will be active in this computer.

Application Types

The Application Types defined in the Deep Security Manager are displayed here. Their properties can be edited globally or for this Security Profile only.

SSL Configurations

Deep Security Manager supports DPI analysis of SSL traffic. The SSL Configurations screen allows you to create SSL Configurations for a given certificate-port pair on one or more interfaces. Certificates can be imported in **P12** or **PEM** format and Windows computers have the option of using **Windows CryptoAPI** directly.

To create a new SSL Configuration, click **New** and follow the steps in the **SSL Configuration** wizard.

If the computer you are configuring is being installed on the computer hosting the Deep Security Manager, the wizard will provide let you use credentials already stored in the Deep Security Manager.

Double-click an existing configuration to display its **Properties** window.

Assignment

- **General Information:** The name and description of the SSL configuration, and whether it is enabled on this computer.
- **Interface Assignments:** Which interfaces this configuration is being applied to.
- **IP Assignment:** Which IP(s) this configuration applies to.
- **Port Selection:** Which port(s) this configuration applies to.

Credentials

The **Credentials** tab lists the current credentials, and has an **Assign New Credentials...** button which lets you change them.

Filtering of SSL traffic is only supported by the Deep Security Agent, not the Deep Security Appliance. The Agent does not support filtering SSL connections on which SSL compression is implemented.

For information on setting up SSL filtering, see Filter SSL Data Streams.

Integrity Monitoring (Events and Rules)

The Integrity Monitoring engine for this computer inherits its **Real Time**, **On**, or **Off** state and its Recommendation Scan behavior from its Security Profile or from the global setting in the Deep Security Manager unless you choose to override it.

Events

Integrity Monitoring Events are displayed the same way as they are in the main Deep Security Manager window except that only events relating to this computer are displayed.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Rules

The Integrity Monitoring Rules defined in the Deep Security Manager are displayed here. Select which ones will be active on this computer.

Log Inspection

The Log Inspection engine for this computer inherits its on or off state and it Recommendation Scan behavior from its Security Profile or from the global setting in the Deep Security Manager unless you choose to override it.

Events

Log Inspection Events are displayed the same way as they are in the main Deep Security Manager window except that only events relating to this computer are displayed.

Rules

The Log Inspection Rules defined in the Deep Security Manager are displayed here. Select which ones will be active on this computer.

Decoders

The Log Inspection Rules included with Deep Security Manager require "1002791 - Default Decoders" to function. Users should not have to write their own decoders.

System

Events

System Events are displayed the same way as they are in the main Deep Security Manager window except that only events relating to this computer are displayed.

System Settings

All System Settings from the Deep Security Manager that can be overridden on specific computers are displayed here.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Security Profiles

Security Profiles allow common configurations of Firewall Rules, Stateful Configurations, and DPI Rules, (with interface assignments for each), to be saved for easy assignment to multiple computers. In the main **Security Profiles** screen, you will see a list of existing profiles. From here you can:

- Create **New** Security Profiles from scratch (New)
- **Import** Security Profiles from an XML file ( )

Do not import Security Profiles from a newer Security Update into a system running an older Security Update. The new Security Profile may reference rules that do not exist in the older version. Always make sure your Security Updates are current.

- Examine or modify the **Properties** of an existing Security Profile ( )
- **Duplicate** (and then modify and rename) an existing Security Profile ( )
- **Delete** a Security Profile ( )
- **Export** a Security Profile to an XML file ( )

Clicking **New** (New) opens the **Security Profiles** wizard which will prompt you for the name of the new profile and then give you the option of opening the **Security Profile Details window**. Clicking **Details** ( ) displays the **Security Profile Details** window.

You can create a new Security Profile based on a Recommendation Scan of a computer. To do so, select a computer and run a Recommendation Scan. (Right-click the computer on the **Computers** screen and select **Actions > Scan for Recommendations**). When the scan is complete, return to the **Security Profiles** screen and click **New** to display the **New Security Profile** wizard. When prompted, choose to base the new Security Profile on "an existing computer's current configuration". Then select "Recommended Application Types and DPI Rules", "Recommended Integrity Monitoring Rules", and "Recommended Log Inspection Rules" from among the computer's properties.

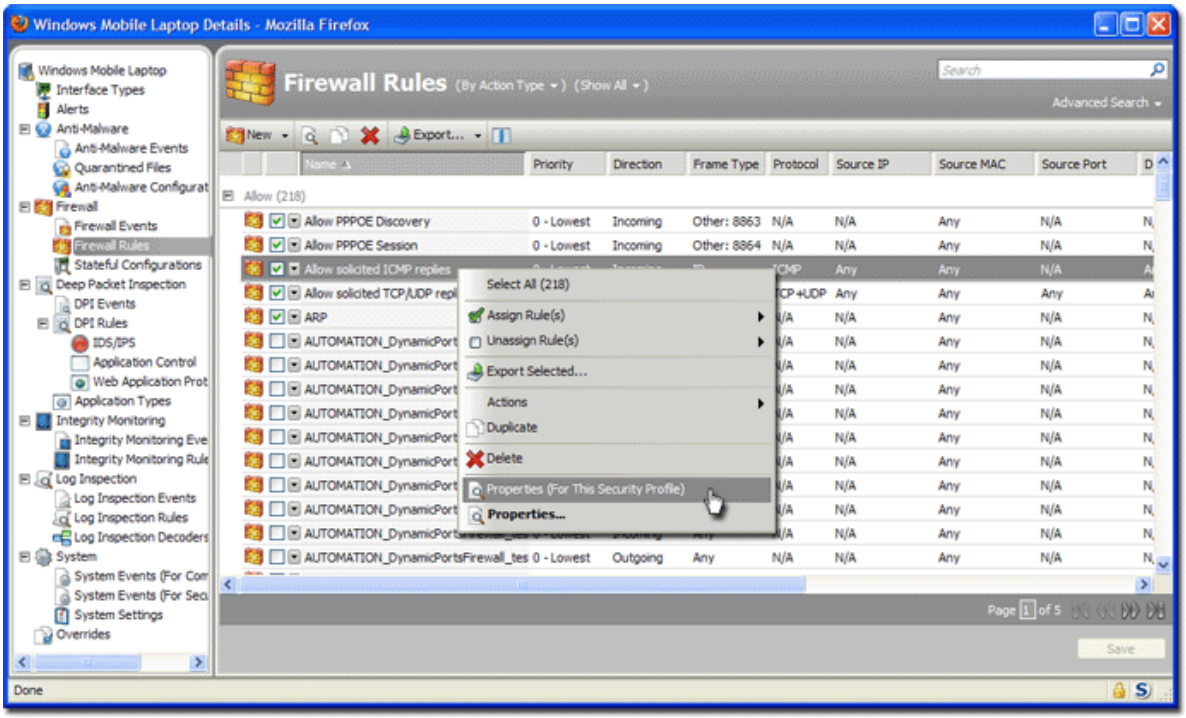
Note that the Security Profile will consist only of recommended elements on the computer, regardless of what Rules are currently assigned to that computer.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Security Profile Details

Whereas the main Deep Security Manager window serves to manage and organize the elements of the whole Deep Security system, the Security Profile **Details** window is used to select available elements from the Deep Security Manager and apply them to the particular Security Profile.

The Security Profile **Details** window is very similar to the main Deep Security Manager window except that all elements in the Security Profile Details screen apply specifically to the Security Profile. By default, all settings are inherited from the global settings of the main Deep Security Manager window. Changes can be made in the Security Profile window that will apply only to this Security Profile. When modifying the properties of an element in the main Deep Security Manager window (Firewall Rule, DPI Rule, etc.), the only option is to modify the "Properties". When modifying the properties of an element in the Security Profile Details window, an additional option is available: "Properties (For This Security Profile)".

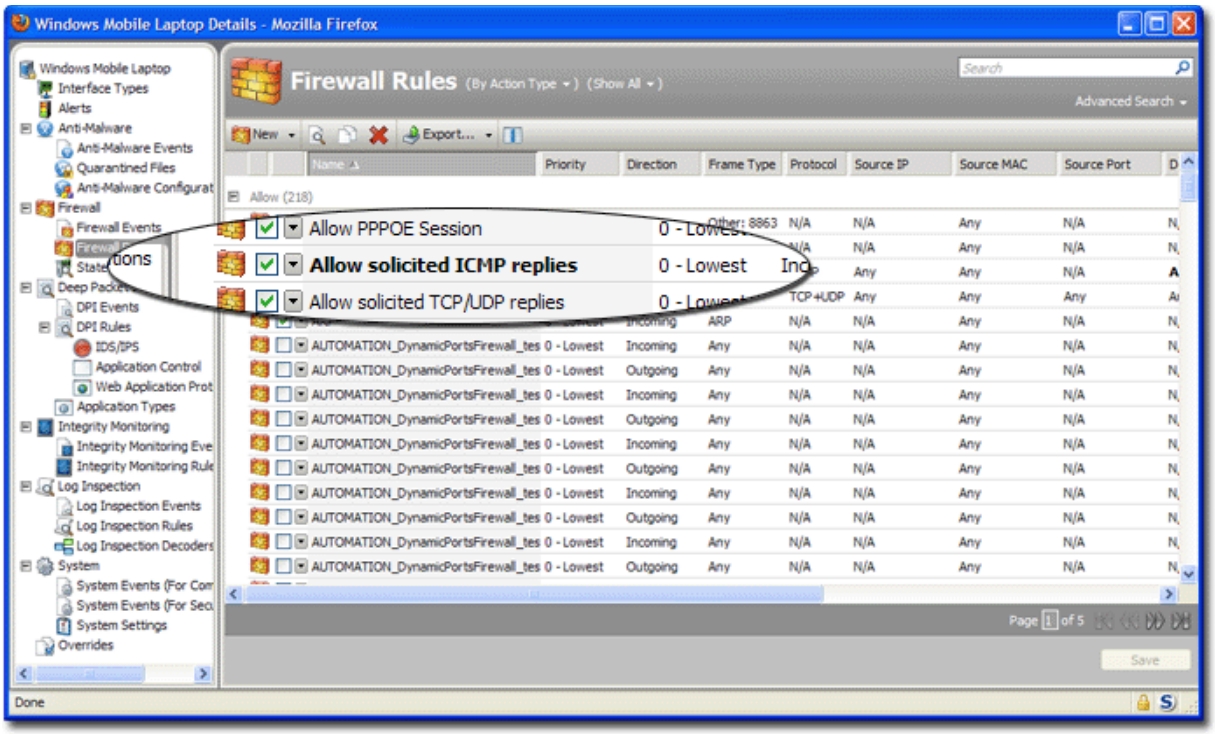


If you edit the "Properties (For this Security Profile)", the changes will only affect that element when it is applied to a computer by this Security Profile.

If you edit the "Properties", the changes will affect the element globally (except where it has been overridden elsewhere).

An element whose properties have been edited "For This Security Profile" will appear in bold letters in the Task Pane to indicate that it has special properties when applied to a computer as a part of this Security Profile.

© Copyright 2011 Trend Micro Inc.
All rights reserved.



Interface Types

If you have computers with more than one interface, you can assign various elements of a Security Profile (Firewall Rules, etc.) to each interface. To configure a Security Profile for multiple interfaces, select **Multiple Interface Assignments** and type names and pattern matching strings in the fields below.

The interface type name is used only for reference. Common names include "LAN", "WAN", "DMZ", and "Wi-Fi" though any name may be used to map to your network's topology.

The Matches defines a wild-card based interface name match to auto map the interfaces to the appropriate interface type. Examples would be "Local Area Connection *", "eth*", and "Wireless *". When an interface cannot be mapped automatically, an alert is triggered. You can manually map it from the **Interfaces** screen in the computer's **Details** window.

If interfaces are detected on the computer which don't match any of these entries, the Manager will trigger an alert.

Alerts

Alerts are displayed the same way as they are in the main Deep Security Manager window except that only alerts relating to computers using this Security Profile are displayed. When an Alert is dismissed here, it is also dismissed in the main Deep Security Manager window.

Anti-Malware

You can set the Security Profile to inherit the global On/Off configuration from the Deep Security Manager or you can uncheck **Inherit** and set the status independently of the global setting.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Anti-Malware Events

Anti-Malware Events are displayed the same way they are in the main Deep Security Manager window except that only events relating to computers using this Security Profile are displayed.

Quarantined Files

Quarantined files are displayed the same way they are in the main Deep Security Manager window except that only files having been found on computers using this Security Profile are displayed.

Anti-Malware Configurations

Real-Time Scan Settings

By assigning an Anti-Malware Configuration here, you are enabling Real-Time Scan mode for computer to which this Security Profile is assigned. Up to five Anti-Malware Configurations can be applied to computers via a Security Profile. They are applied in order of priority and according to the schedule during which they are active.

"No Schedule" means the configuration will never be active.

Manual Scan Settings

Select the Anti-Malware Configuration to use when manually initiating a scan.

Scheduled Scan Settings

Select the Anti-Malware Configuration to use when a running a scan that is initiated by a Scheduled Task.

Firewall (Events, Rules, and Stateful Configurations)

The Firewall for this Security Profile inherits its on or off state from the global setting in the Deep Security Manager unless you choose to override it.

Note that if a Security Profile with Firewall turned off is applied to a computer and that computer is set to inherit firewall settings, all Firewall elements (Firewall Rules and Stateful Configurations) will be turned off on that computer, even elements that were assigned directly to the computer before the Security Profile was applied.

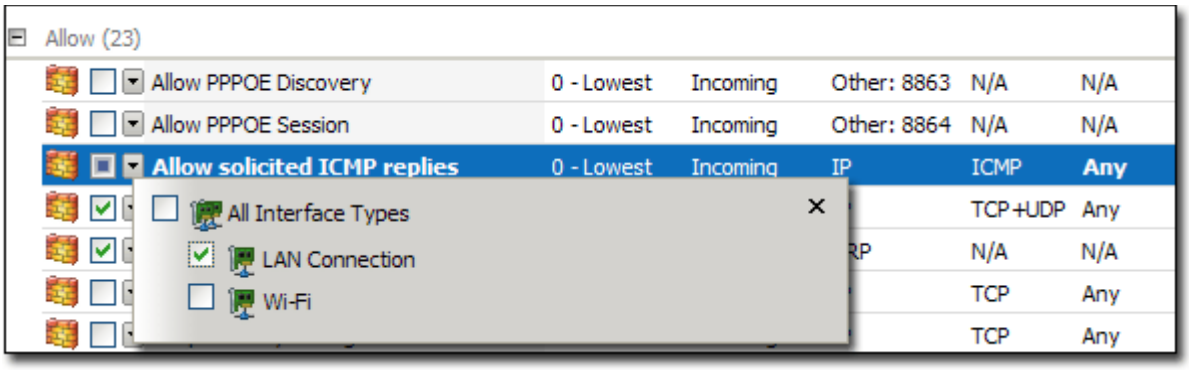
Events

Firewall Events are displayed the same way as they are in the main Deep Security Manager window except that only events relating to computers using this Security Profile are displayed.

Rules

The Firewall Rules defined in the Deep Security Manager are displayed here. Select which ones will be active in this Security Profile. If you have defined multiple Interfaces for this Profile (above), use the gray drop-down menu to select whether the Firewall Rule will apply to all interfaces or to specific ones only.

© Copyright 2011 Trend Micro Inc.
All rights reserved.



Stateful Configurations

Select which Stateful Configuration to apply to this Security Profile. If you have defined multiple Interfaces for this Profile (above), you can specify independent configurations for each interface.

Deep Packet Inspection (Events, Rules and Application Types)

The DPI engine for this Security Profile inherits its on or off state, its Inline behavior, and it Recommendation Scan behavior from the Global or Security Profile setting unless you choose to override them.

Events

DPI Events are displayed the same way as they are in the main Deep Security Manager window except that only events relating to computers using this Security Profile are displayed.

Rules

The DPI Rules defined in the Deep Security Manager are displayed here. Select which ones will be active in this Security Profile. If you have defined multiple Interfaces for this Profile (above), use the gray drop-down menu to select whether the DPI Rule will apply to all interfaces or to specific ones only.

Application Types

The Application Types defined in the Deep Security Manager are displayed here. As with other elements at the Security Profile level, their properties can be edited globally or for this Security Profile only.

Integrity Monitoring (Events and Rules)

Integrity Monitoring: The Integrity Monitoring engine for this Security Profile inherits its **Real Time**, **On**, or **Off** state from the Global or Security Profile setting unless you choose to override it.

Integrity Scan: Click **Scan For Integrity Changes** to carry on an on-demand Integrity Scan.

Baseline: The Baseline is the original secure state that an Integrity Scan's results will be compared against. Click **Rebuild Baseline** to create a new Baseline for Integrity Scans. Click **View Baseline** to view the current Baseline data.

Recommendations: Displays when the last Recommendation Scan occurred and number of recommended Integrity Monitoring Rules. Whether Rules are assigned or not is inherited

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Events

Integrity Monitoring Events are displayed the same way as they are in the main Deep Security Manager window except that only events relating to computers using this Security Profile are displayed.

Rules

The Integrity Monitoring Rules defined in the Deep Security Manager are displayed here. Select which ones will be active in this Security Profile.

Log Inspection

The Log Inspection engine for this Security Profile inherits its on or off state and it Recommendation Scan behavior from the Global or Security Profile setting unless you choose to override it.

Events

Log Inspection Events are displayed the same way as they are in the main Deep Security Manager window except that only events relating to computers using this Security Profile are displayed.

Rules

The Log Inspection Rules defined in the Deep Security Manager are displayed here. Select which ones will be active in this Security Profile.

Decoders

The Log Inspection Rules included with Deep Security Manager require "1002791 - Default Decoders" to function. Users should not have to write their own decoders

System

Events (For Computers)

System Events are displayed the same way as they are in the main Deep Security Manager window except that only events relating to computers using this Security Profile are displayed.

Events (For Security Profile)

System Events for this Security Profile (if it was created, modified, etc.) are displayed here.

System Settings

All System Settings from the Deep Security Manager that can be overridden on specific Security Profiles are displayed here.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Anti-Malware

At the global level, Anti-Malware protection can be turned on or off. However, this setting can be overridden at the Security Profile and Computer level.

The Deep Security Manager provides Anti-Malware protection with the following capabilities:

- Anti-Malware protection to active virtual machines running within a VMware vShield Endpoint Security environment.
- Customizable Anti-Malware Configurations that are applied to Security Profiles and computers.
- Real-time, manual, and scheduled scanning.
- Smart Scan server support.
- Quarantined file management, including the ability to download and delete files using the Deep Security Manager.
- Anti-Malware Web service integration.

Once Anti-Malware protection is enabled, file-based scans are carried out to ensure protected computers are malware free. Scanning is performed by the Deep Security Virtual Appliance. It is not necessary to install Agents on the computers being scanned.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Anti-Malware Events

By default, the Deep Security Manager collects Anti-Malware Event logs from the Virtual Appliances at every heartbeat. The data from the logs is used to populate the various reports, graphs, and charts in the Deep Security Manager.

Once collected by the Deep Security Manager, Event logs are kept for a period of time which can be set from **System** tab in the **System > System Settings** screen.

From the main screen you can:

- **View** ( ) the properties of a particular event.
- **Filter the list.** Use the **Period** and **Computer** toolbars to filter the list of events.
- **Export** ( ) the event list data to a CSV file.
- **Search** ( ) for a particular event.

Additionally, right-clicking a log entry gives you the option to:

- **Add Tag(s)** to this event (See Event Tagging in the **Reference** section.)
- **Remove Tag(s)** from this event.
- View the **Computer Details** screen of the computer that generated the log entry.
- View **Quarantined File Details** of the file associated with this event. (Only available if the action associated with this event was quarantined.)

Columns for the Anti-Malware Events display:

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Infected File:** The location and name of the infected file.
- **Tag(s):** Event tags associated with this event.
- **Malware:** The name of the malware that was found.
- **Scan Type:** The type of scan that found the malware (Real-Time, Scheduled, or Manual).
- **Result:** Displays the results of the actions specified in the Anti-Malware Configuration associated with event.
    - **Cleaned:** Deep Security successfully terminated processes or deleted registries, files, cookies, or shortcuts, depending on the type of malware.
    - **Clean Failed:** Malware could not be cleaned for a variety of possible reasons.
    - **Deleted:** An infected file was deleted.
    - **Delete Failed:** An infected file could not be deleted for a variety of possible reasons. For example, the file may be locked by another application, is on a CD, or is in use. If possible, Deep Security will delete the infected file once it is released.
    - **Quarantined:** An infected file was moved to the quarantine folder on the Appliance.
    - **Quarantine Failed:** An infected file could not be quarantined for a variety of possible reasons. For example, the file may be locked by another application, is on a CD, or is in use. If possible, Deep Security will quarantine the infected file once it is released. It is also possible that file exceeded the maximum quarantined file size settings on the **System > System Settings > Anti-Malware** screen.
    - **Access Denied:** Deep Security has prevented the infected file from being accessed without removing the file from the system.
    - **Passed:** Deep Security did not take any action but logged the detection of the malware.
- **Event Origin:** Indicates from which part of the Deep Security System the event originated. For Anti-Malware Events, this will always be the Appliance.
- **Reason:** The Anti-Malware Configuration that was in effect when the malware was detected.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

View Event Properties

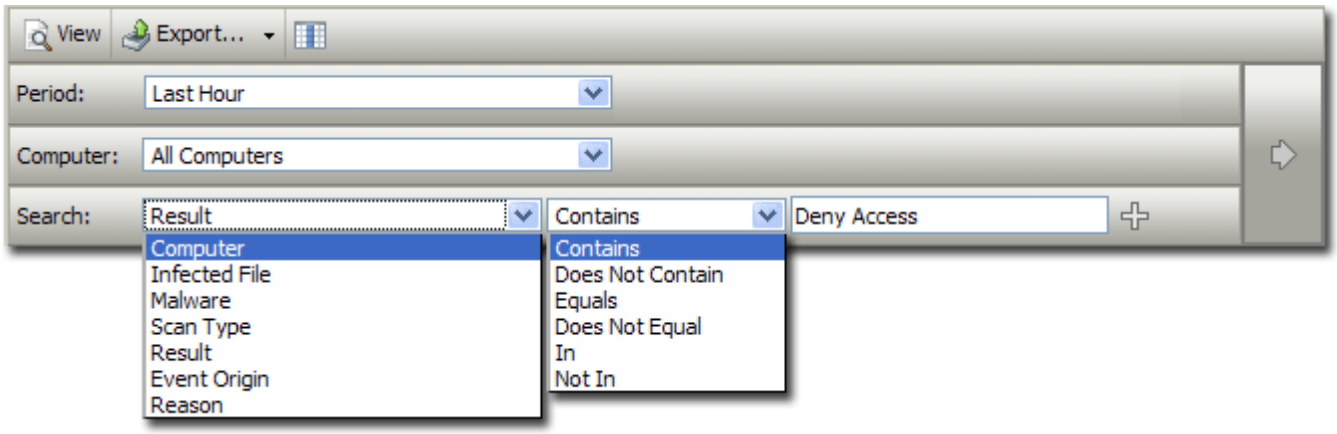
Double-clicking an event (or selecting **View** from the context menu) displays the **Properties** window for that entry which displays all the information about the event on one screen. The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **System > System Settings > Tags**, and Event Tagging in the **Reference** section.

Filter the List and/or Search for an Event

Selecting "Open Advanced Search" from the "Advanced Search" drop-down menu toggles the display of the advanced search options.

The **Period** toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The **Computers** toolbar lets you organize the display of event log entries by computer groups or computer Security Profiles.



Advanced Search functions (searches are not case sensitive):

- **Contains:** The entry in the selected column contains the search string
- **Does Not Contain:** The entry in the selected column does not contain the search string
- **Equals:** The entry in the selected column exactly matches the search string
- **Does Not Equal:** The entry in the selected column does not exactly match the search string
- **In:** The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In:** The entry in the selected column does not exactly match any of the comma-separated search string entries

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the toolbars with the right-arrow on it).

Export...

Clicking **Export...** exports all or selected events to a CSV file.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Quarantined Files

A Quarantined File is a file that has been found to be or to contain malware and has therefore been encrypted and moved to a special folder on the Appliance. ("Quarantine" is a scan action that you can specify when creating an Anti-Malware Configuration.) Once the file has been identified and quarantined, you can chose to download it to your computer in a encrypted and compressed format. Whether or not an infected file is quarantined depends on the Anti-Malware Configuration that was in effect when the file was scanned.

After the quarantined file has been downloaded to your computer, the **Quarantined File** wizard will display a link to an **Administration Utility** which you can use to decrypt, examine, and restore the file.

A limited amount of disk space is set aside for storing quarantined files. The amount of space can be configured in **System > System Settings > Anti-Malware > Quarantined Files**. Alerts are raised when there is not enough disk space to quarantine a suspicious file.

Quarantined files will be automatically deleted from a Virtual Appliance under the following circumstances:

- If a VM undergoes vMotion, quarantined files associated with that VM will be deleted from the Virtual Appliance.
- If a VM is deactivated from the Deep Security Manager, quarantined files associated with that VM will be deleted from the Virtual Appliance.
- If a Virtual Appliance is deactivated from the Deep Security Manager, all the quarantined files stored on that Virtual Appliance will be deleted.
- If a Virtual Appliance is deleted from the vCenter, all the quarantined files stored on that Virtual Appliance will also be deleted.

The **Anti-Malware Quarantined Files** screen allows you to manage quarantine tasks. Using the menu bar or the right-click context menu, you can:

- View the **Details** ( ) of a quarantined file.
- **Download Quarantined File(s)** ( ) Move quarantined files from the Virtual Appliance to a location of your choice.
- **Delete Quarantined File(s)** ( ) Delete one or more quarantined files from the Virtual Appliance.
- **Add or Remove Columns** ( ) columns can be added or removed by clicking **Add/Remove.**
- **Search** ( ) for a particular quarantined file.

Details

The Quarantined File **Details** screen displays more information about the file and lets you download the quarantined file to your computer or delete it where it is.

- **Date/Time:** Time (on the infected computer) that the infection was detected.
- **Infected File:** The name of the infected file.
- **Malware:** The name of the malware that was found.
- **Computer:** The computer on which this file was found. (If the computer has been removed, this entry will read "Unknown Computer".)

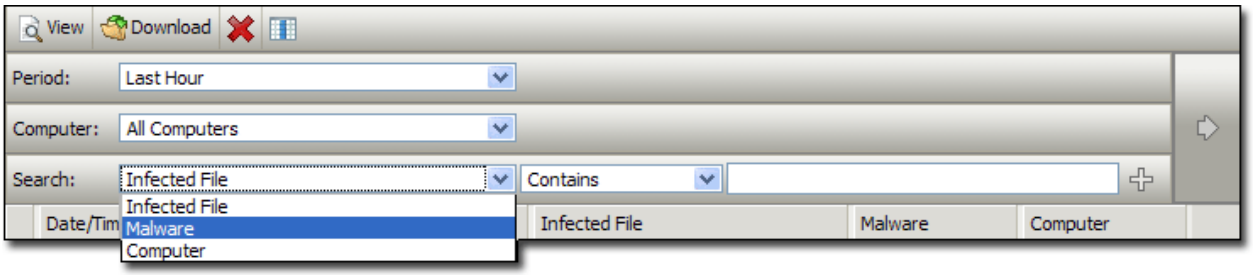
© Copyright 2011 Trend Micro Inc.
All rights reserved.

Filter the List and/or Search for a Quarantined File

The **Period** tool bar allows you to filter the list to display only those files quarantined within a specific time frame.

The **Computers** tool bar allows you to organize the display of quarantined file entries by Computer Groups or Computer Security Profiles.

Selecting "Open Advanced Search" from the "Advanced Search" drop-down menu toggles the display of the advanced search options:



Advanced Search functions (searches are not case sensitive):

- **Contains:** The entry in the selected column contains the search string.
- **Does Not Contain:** The entry in the selected column does not contain the search string.
- **Equals:** The entry in the selected column exactly matches the search string.
- **Does Not Equal:** The entry in the selected column does not exactly match the search string.
- **In:** The entry in the selected column exactly matches one of the comma-separated search string entries.
- **Not In:** The entry in the selected column does not exactly match any of the comma-separated search string entries.

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the tool bars with the right-arrow on it).

- **Infected File:** Shows the name of the infected file and the specific security risk.
- **Malware:** Names the malware infection.
- **Computer:** Indicates the name of the computer with the suspected infection.

Manually Restoring Quarantined Files

To manually restore a quarantined file, you must use the quarantined file decryption utility to decrypt the file and then move it back to its original location. The decryption utility is in a zip file, QFAdminUtil.zip, located in the "util" folder under the Deep Security Manager root directory. The zipped file contains two utilities which perform the same function: QDecrypt.exe and QDecrypt.com. Running QDecrypt.exe invokes an open file dialog that lets you select the file for decryption. QDecrypt.com is a command-line utility with the following options:

- **/h, --help**: show this help message
- **--verbose**: generate verbose log messages
- **/i, --in=<str>**: quarantined file to be decrypted, where **<str>** is the name of the quarantined file
- **/o, --out=<str>**: decrypted file output, where **<str>** is the name given to the resulting decrypted file

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Anti-Malware Configuration

Deep Security allows you to create a variety of Anti-Malware Configurations to automatically handle the way the detection of malware is processed. Configuration options include what files to scan, whether the scanning is done in real time or on a scheduled basis, and what actions to carry out if malware is detected. This screen lets you define global Anti-Malware Configurations. How, in what combination, and when these configurations are in effect on a computer is set at the Security Profile and at the computer levels. Also, as with most elements in Deep Security, many global settings can be overridden at the Security Profile and computer levels. (See Inheritance and Overrides in the **Reference** section.)

From the global **Anti-Malware Configuration** screen you can:

- Create **New** ( ) configurations or import an existing configuration from an external source.
- View the **Properties**( ) of an Anti-Malware configuration.
- **Duplicate** ( ) (and then modify) existing file configurations.
- **Delete** ( ) the highlighted configuration file from the configuration list.
- **Export** ( ) the displayed or selected configuration to a CSV file.
- **Add or Remove Columns** ( ) from the display**.**
- **Search** ( ) for a particular configuration file.

Properties

General

General Information

- Name and description of the Anti-Malware Configuration.

Scan Settings

- **Folders to scan:** Specify which folders to scan for malware.
- **Files to scan:** Specify which files to scan for malware.

Intelliscan is a method of identifying which files to scan that is more efficient than the standard "scan all files" option, though inherently less secure since it does not "scan all files". For executable files (that is, .zip, .exe), the true file type is determined from the file content. In the event that a file is not executable (i.e. txt), Intelliscan will use the file header to verify the true file type.

Exclusions

Allows you to exclude specific directories, files, and file extensions from being scanned. For example, if ScanMail for Exchange (SMEX) protects an MS Exchange server on the VM, you might want to exclude the SMEX quarantine folder to avoid re-scanning files that have already been confirmed to be malware.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Actions

Upon detection

You can instruct Deep Security to automatically decide which actions to take by selecting the **Use ActiveAction** option.

ActiveAction is a set of pre-configured actions that are performed on viruses and other types of malware. Use ActiveAction if you are not sure which scan action is suitable for each type of virus/malware .ActiveAction scan actions are updated along with virus pattern updates.

Malware Type	Real-Time Scan		Manual Scan or Scheduled Scan	
	First Action	Second Action	First Action	Second Action
Joke	Quarantine	Delete	Quarantine	Delete
Trojan	Quarantine	Delete	Quarantine	Delete
Virus	Clean	Quarantine	Clean	Quarantine
Test Virus	Deny Access	N/A	Pass	N/A
Spyware	Quarantine	Delete	Quarantine	Delete
Packer	Quarantine	N/A	Quarantine	N/A
Possible malware	Pass	N/A	Pass	N/A
Others	Clean	Quarantine	Clean	Quarantine

Alternatively, you can manually specify a sequence of actions you want Deep Security to take. There are four possible actions that Deep Security can take when it encounters an infected file:

1. **Pass:** Allows full access to the infected file without doing anything to the file.
2. **Delete:** Deletes the infected file.
3. **Quarantine:** Moves the file to the quarantine directory on the Virtual Appliance. (Once quarantined, you can download the file to a location of your choice. See **Anti-Malware > Quarantined Files** for more information.)
4. **Clean:** Cleans a cleanable file before allowing full access to the file.
5. **Deny Access:** This scan action can only be performed during Real-time scans. When Deep Security detects an attempt to open or execute an infected file, it immediately blocks the operation. If an Anti-Malware configuration with the "Deny Access" option selected is applied during a Manual or Scheduled scan, a "Pass" action will be applied and an Anti-Malware Event will be recorded.

If you manually select a scan action and choose Clean, you need to specify a second action for Deep Security to take if cleaning is unsuccessful.

Unscannable files

Select an action to take if a file is unscannable. A file may be unscannable for a variety of reasons including being password protected, being compressed with an unsupported format, or being corrupted.

Possible malware

Select an action to take if a file is identified as possible malware. Possible malware is a file that appears suspicious but cannot be classified as a specific malware variant. If you leave this option set to "Unspecified", the action will that selected in **Upon Detection**, above. When possible malware is detected, Trend Micro recommends that you contact your support provider for assistance in further analysis of the file.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Options

General Options

- **Enable Spyware/Grayware Scan:** The Spyware Scan Engine scans for Spyware/Grayware and performs the actions specified on the **Actions** tab.
- **Scan Compressed Files:** Specify under what conditions to scan a file and whether to scan compressed files.

A file or group of files can undergo more than one round of compression. The **Maximum Layers** options lets you specify through how many layers of compression you want Deep Security to scan. Note that scanning large files with multiple layers of compression can affect performance.

Real-Time Options

- **Enable IntelliTrap:** Virus writers often attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of such viruses entering your network by blocking real-time compressed executable files and pairing them with other malware characteristics. (Intellitrap only works in Real-Time mode.)
- **Scan files when:** Choose between scanning files only when they are opened for reading, or when they are opened for both reading and writing.

Because IntelliTrap identifies such files as security risks and may incorrectly block safe files, consider quarantining (not deleting or cleaning) files when you enable IntelliTrap. If users regularly exchange real-time compressed executable files, disable IntelliTrap.

IntelliTrap uses the following Anti-Malware components:

- Virus Scan Engine
- IntelliTrap Pattern
- IntelliTrap Exception Pattern

Alert

Select whether an alert is raised if this Anti-Malware Configuration triggers an event.

Assigned To

Indicates which Security Profile(s) and computer(s) are using this particular Anti-Malware configuration.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Firewall

Turn the Firewall on or off.

The information area will tell you whether the network engine is operating Inline or in Tap mode. When operating Inline, the live packet stream passes through the network engine. Stateful tables are maintained, Firewall Rules are applied and traffic normalization is carried out so that DPI Rules can be applied to payload content. When operating in Tap Mode, the live packet stream is cloned and diverted from the main stream. In Tap Mode, the live packet stream is not modified; all operations are carried out on the cloned stream.

To switch between Inline and Tap mode, go to **System > System Settings > Firewall and DPI**.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Firewall Events

By default, the Deep Security Manager collects Firewall and DPI Event logs from the Deep Security Agents/Appliances at every heartbeat. (This can be turned off from the **Firewall and DPI** tab in the **System > System Settings** screen.) The data from the logs is used to populate the various reports, graphs, and charts in the Deep Security Manager.

Once collected by the Deep Security Manager, Event logs are kept for a period of time which can be set from **System** tab in the **System > System Settings** screen.

Firewall Event icons:

- Single Event
- Single Event with data
- Folded Event
- Folded Event with data

Event folding occurs when multiple events of the same type occur in succession. This saves disk space and protects against DoS attacks that may attempt to overload the logging mechanism.

From the main screen you can:

- **View** ( ) the properties of a particular event
- **Filter the list:** Use the **Period** and **Computer** toolbars to filter the list of events
- **Export** ( ) the event list data to a CSV file
- **Search** ( ) for a particular event

Additionally, right-clicking a log entry gives you the option to:

- **Add Tag(s):** Add an Event Tag to this event (See Event Tagging in the **Reference** section.)
- **Remove Tag(s):** Remove exiting event Tags
- **Computer Details:** View the Details screen of the computer that generated the log entry
- **Firewall Rule Properties:** View the properties of the Firewall Rule associated with this event
- **Whois Source IP:** Perform a whois on the source IP
- **Whois Destination IP:** Perform a whois query on the destination IP

Columns for the Firewall Events display:

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Reason:** Log entries on this screen are generated either by Firewall Rules or by Stateful Configuration settings. If an entry is generated by a Firewall Rule, the column entry will be prefaced by "Firewall Rule:" followed by the name of the Firewall Rule. Otherwise the column entry will display the Stateful Configuration setting that generated the log entry. (For a listing of possible packet rejection reasons, see "Packet Rejection Reasons" in the **Reference** section.)
- **Action:** The action taken by the Firewall Rule or Stateful Configuration. Possible actions are: Allow, Deny, Force Allow, and Log Only.
- **Rank:** The Ranking system provides a way to quantify the importance of DPI and Firewall Events. By assigning "asset values" to computers, and assigning "severity values" to DPI Rules and Firewall Rules, the importance ("Rank") of an Event is calculated by multiplying the two values together. This allows you to sort Events by Rank when viewing DPI or Firewall Events.
- **Direction:** The direction of the affected packet (incoming or outgoing).

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **Interface:** The MAC address of the interface through which the packet was traveling.
- **Frame Type:** The frame type of the packet in question. Possible values are "IP", "ARP", "REVARP", and "Other: XXXX" where XXXX represents the four digit hex code of the frame type.
- **Protocol:** Possible values are "ICMP", "IGMP", "GGP", "TCP", "PUP", "UDP", "IDP", "ND", "RAW", "TCP+UDP", AND "Other: nnn" where nnn represents a three digit decimal value.
- **Flags:** Flags set in the packet.
- **Source IP:** The packet's source IP.
- **Source MAC:** The packet's source MAC address.
- **Source Port:** The packet's source port.
- **Destination IP:** The packet's destination IP address.
- **Destination MAC:** The packet's destination MAC address.
- **Destination Port:** The packet's destination port.
- **Packet Size:** The size of the packet in bytes.

Log-only rules will only generate a log entry if the packet in question is not subsequently stopped either by a **deny** rule, or an **allow** rule that excludes it. If the packet is stopped by one of those two rules, *those* rules will generate a log entry and *not* the **log-only** rule. If no subsequent rules stop the packet, the log-only rule will generate an entry.

View Event Properties

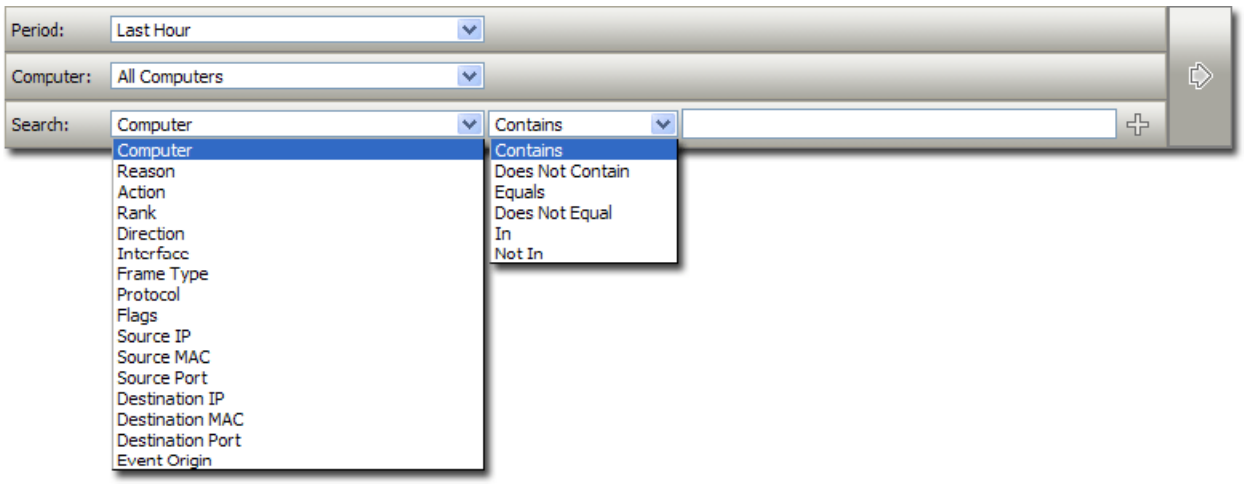
Double-clicking an event displays the **Properties** window for that entry which displays all the information about the event on one screen. The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **System > System Settings > Tags**, and Event Tagging in the **Reference** section.

Filter the List and/or Search for an Event

Selecting "Open Advanced Search" from the "Advanced Search" drop-down menu toggles the display of the advanced search options.

The **Period** toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The **Computers** toolbar lets you organize the display of event log entries by computer groups or computer Security Profiles.



© Copyright 2011 Trend Micro Inc.
All rights reserved.

Advanced Search functions (searches are not case sensitive):

- **Contains:** The entry in the selected column contains the search string
- **Does Not Contain:** The entry in the selected column does not contain the search string
- **Equals:** The entry in the selected column exactly matches the search string
- **Does Not Equal:** The entry in the selected column does not exactly match the search string
- **In:** The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In:** The entry in the selected column does not exactly match any of the comma-separated search string entries

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the toolbars with the right-arrow on it).

Export…

Clicking the **Export...** button exports all or selected events to a CSV file.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Firewall Rules

Firewall Rules examine the control information in individual packets. The Rules either block or allow those packets based on rules that are defined on these screens. Firewall Rules are assigned directly to computers or to Security Profiles which are in turn assigned to a computer or collection of computers.

Solaris Agents will only examine packets with an IP frame type, and Linux Agents will only examine packets with IP or ARP frame types. Packets with other frame types will be allowed through. Note that the Virtual Appliance does not have these restrictions and can examine all frame types, regardless of the operating system of the virtual machine it is protecting.

Firewall Rule icons:

- Normal Firewall Rules
- Firewall Rules that operate according to a schedule

From the main screen you can:

- Create **New** Firewall Rules from scratch (New)
- **Import** ( ) Firewall Rules from an XML file
- Examine or modify the **Properties** of an existing Firewall Rule ( )
- **Duplicate** (and then modify) existing Firewall Rules ( )
- **Delete** a Firewall Rule ( )
- **Export** ( ) one or more Firewall Rules to an XML file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Firewall Rules that are assigned to one or more computers or that are part of a Security Profile cannot be deleted.

Clicking **New** (New) or Properties ( ) displays the **Firewall Rules Properties** window.

Firewall Rule Properties

General Information

- **Name:** The name of the Firewall Rule.
- **Description:** A detailed description of the Firewall Rule.
- **Action:** Your Firewall Rule can behave in four different ways. These are described here in order of precedence:
    1. The traffic can **bypass** the firewall completely. This is a special rule that can cause the packets to bypass the firewall and DPI engine entirely. Use this setting for media intensive protocols where filtering may not be desired. To find out more about the **bypass** rule, see "Bypass Rule" in the **Reference** section.
    2. It can **log only**. This means it will only make an entry in the logs and not interfere with the traffic.
    3. It can **force allow** defined traffic (it will allow traffic defined by this rule *without* excluding any other traffic.)
    4. It can **deny** traffic (it will deny traffic defined by this rule.)
    5. It can **allow** traffic (it will *exclusively* allow traffic defined by this rule.)

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Only one rule action is applied to any particular packet, and rules (of the same priority) are applied in the order listed above.

- **Priority:** If you have selected "force allow", "deny", or "log only" as your rule action, you can set a priority here of 0 (low) to 4 (highest). Setting a priority allows you to combine the actions of rules to achieve a cascading rule effect. **Log only** rules can only have a priority of **4**, and **Allow** rules can only have a priority of **0**.

The priority determines the order in which rules are applied. High priority rules get applied before low priority rules. For example, a port 80 incoming deny rule with a priority of 3 will drop a packet before a port 80 incoming force allow rule with a priority of 2 ever gets applied to it.

- **Packet Direction:** Select whether this rule will be applied to **incoming** or **outgoing** traffic.
- **Frame Type:** Select or specify the frame type your rule will be looking for. Use the checkbox to specify whether you will be filtering *for* this frame type or *anything but* this frame type.

For a list of frame types, see the Internet Assigned Numbers Authority (IANA) Web site.

- **Protocol:** Select or specify the protocol your rule will be looking for. Use the checkbox to specify whether you will be filtering *for* this protocol or *anything but* this protocol.

Note that you can choose from the drop down list of predefined common protocols, or you can select "Other" and enter the protocol code yourself (a three digit decimal value from 0 to 255).

Packet Source

The following options apply to the packet header's source information:

- **IP:** Specify an IP address, a masked IP address, an IP range, or select an IP list from one you defined in the **IP Lists** screen.
- **MAC:** Specify a MAC address or select a MAC list from one you defined in the **MAC Lists** screen.
- **Port:** You can specify a comma separated list of ports or a dash separated port range in the port(s) option as well as just a single port (e.g., 80, 443, 1-100) or select a Port list from one you defined in the **Port Lists** screen.

Packet Destination

The following options apply to the packet header's destination information:

- **IP:** Specify an IP address, a masked IP address, an IP range, or select an IP list from one you defined in the **IP Lists** screen.
- **MAC:** Specify a MAC address or select a MAC list from one you defined in the **MAC Lists** screen.
- **Port:** You can specify a comma separated list of ports or a dash separated port range in the port(s) option as well as just a single port (e.g., 80, 443, 1-100) or select a Port list from one you defined in the **Port Lists** screen.

Specific Flags

If you have selected TCP, ICMP, or TCP+UDP as your protocol in the General Information section above, you can direct your Firewall Rule to watch for specific flags.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Options

Alert

Select whether or not this Firewall Rule should trigger an alert when it is triggered. If you only wish this rule to be active during specific periods, assign a schedule from the drop-down list.

Note that only Firewall Rules whose "Action" is set to "Deny" or "Log Only" can be configured to trigger an alert. (This is because alerts are triggered by counters which are incremented with data from log files.)

Schedule

Select whether the Firewall Rule should only be active during a scheduled time.

Firewall Rules that are active only at scheduled times are displayed in the **Firewall Rules** screen with a small clock over their icon ( ).

Context

Rule Contexts are a powerful way of implementing different security policies depending on the computer's network environment. You will most often use Contexts to create Security Profiles which apply different Firewall and DPI Rules to computers (usually mobile laptops) depending on whether that computer is in or away from the office.

Contexts are designed to be associated with Firewall and DPI Rules. If the conditions defined in the Context associated with a Rule are met, the Rule is applied.

To determine a computer's location, Contexts examine the nature of the computer's connection to its domain controller. For more information on Contexts, see **Components > Contexts**.

For an example of a Security Profile that implements Firewall Rules using Contexts, look at the properties of the "Windows Mobile Laptop" Security Profile.

Assigned To

This tab displays a list of Security Profiles which include this Firewall Rule as well as any computers to which this Firewall Rule has been assigned directly. Firewall Rules can be assigned to Security Profiles in the **Security Profiles** screen and to computers in the **Computers** screen.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Stateful Configurations

Deep Security's Stateful Configuration mechanism analyzes each packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols like UDP and ICMP, a pseudo-stateful mechanism is implemented based on historical traffic analysis. Packets are handled by the stateful mechanism as follows:

1. A packet is passed to the stateful routine if it has been allowed through by the static Firewall Rule conditions,
2. The packet is examined to determine whether it belongs to an existing connection by checking a connection table created by the stateful mechanism for matching end points, and
3. The TCP header is examined for correctness (e.g. sequence numbers, flag combinations, etc.).

Stateful Configuration icons:

- Normal Stateful Configurations

The **Stateful Configuration** screen lets you define multiple stateful inspection configurations which you can then include in your Security Profiles. From the toolbar or shortcut menu you can:

- Create **New** (New) Stateful Configurations from scratch
- **Import** ( ) Stateful Configuration from an XML file
- Examine or modify the **Properties** ( ) of an existing Stateful Configuration
- **Duplicate** ( ) (and then modify) existing Stateful Configurations
- **Delete** a Stateful Configuration ( )
- **Export** ( ) one or more Stateful Configurations to an XML file. (Either export them all by click the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking **New** (New) or **Properties** ( ) displays the **Stateful Configuration properties window.**.

Stateful Configuration Properties

General Information

- **Name:** The name of the Stateful Configuration.
- **Description:** Type a description of the Stateful Configuration. This description will only appear here.

IP Packet Inspection

- **Deny all incoming fragmented packets:** If this option is enabled, all fragmented packets are dropped with the following log entry: "IP fragmented packet". The one exception to this rule is the presence of packets with a total length smaller than the IP header length. Such packets are dropped silently.

Attackers sometimes create and send fragmented packets in an attempt to bypass Firewall Rules.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

The Firewall Rule engine, by default, performs a series of checks on fragmented packets. This is default behavior and cannot be reconfigured. Packets with the following characteristics are dropped:

- **Invalid fragmentation flags/offset:** A packet is dropped when *either* the **DF** and **MF** flags in the IP header are set to 1, *or* the header contains the **DF** flag set to 1 and an **Offset** value different than 0.
- **First fragment too small:** A packet is dropped if its **MF** flag is set to 1, its **Offset** value is at 0, and it has total length of less than 120 bytes (the maximum combined header length).
- **IP fragment out of boundary:** A packet is dropped if its **Offset** flag value combined with the total packet length exceeds the maximum datagram length of 65535 bytes.
- **IP fragment offset too small:** A packet is dropped if it has a non-zero **Offset** flag with a value that is smaller than 60 bytes.

TCP

TCP Packet Inspection

- **Deny TCP packets containing CWR, ECE flags:** These flags are set when there is network congestion.

RFC 3168 defines two of the six bits from the Reserved field to be used for ECN (Explicit Congestion Notification), as follows:

- Bits 8 to 15: CWR-ECE-URG-ACK-PSH-RST-SYN-FIN
- TCP Header Flags Bit Name Reference:
  - Bit 8: CWR (Congestion Window Reduced) [RFC3168]
  - Bit 9: ECE (ECN-Echo) [RFC3168]

Automated packet transmission (such as that generated by a denial of service attack, among other things) will often produce packets in which these flags are set.

- **Enable TCP stateful inspection:** Enable stateful inspection at the TCP level. If you enable stateful TCP inspection, the following options become available:
  - **Enable TCP stateful logging:** TCP stateful inspection events will be logged.
  - **Limit the number of incoming connections from a single computer to:** Limiting the number of connections from a single computer can lessen the effect of a denial of service attack.
  - **Limit the number of outgoing connections to a single computer to:** Limiting the number of outgoing connections to a single computer can significantly reduce the effects of Nimda-like worms.
  - **Limit the number of half-open connections from a single computer to:** Setting a limit here can protect you from DoS attacks like SYN Flood. Although most servers have timeout settings for closing half-open connections, setting a value here can prevent half-open connections from becoming a significant problem. If the specified limit for SYN-SENT(remote) entries is reached, subsequent TCP packets from that specific computer will be dropped.

When deciding on how many open connections from a single computer to allow, choose your number from somewhere between what you would consider a reasonable number of half-open connections from a single computer for the type of protocol being used, and how many half-open connections from a single computer your system can maintain without getting congested.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **Enable Syn-Flood protection when the number of half-open connections exceeds:** Unlike setting a hard limit on the number of half-open connections from a single computer, the Syn-Flood protection mechanism starts to use Syn-cookies once the set number of open connections is reached (regardless of whether the connections come a single computer or not). The use of syn-cookies means that connections are not rejected. However, no entry is created for them in the state table, and they are not passed to the application until an appropriate SYN-ACK is received from the destination computer.

The SYN-Flood protection setting applies to Windows Agents and the Virtual Appliance only. It will be ignored by Linux and Solaris Agents.

- **Enable ACK Storm protection when the number of already acknowledged packets exceeds:** Set this option to log an event that an ACK Storm attack has occurred.
  - **Drop Connection when ACK Storm detected:** Set this option to drop the connection if such an attack is detected.

FTP Options

- **Active FTP**
  - **Allow Incoming:** Allow Active FTP when this computer is acting as a server.
  - **Allow Outgoing:** Allow Active FTP when this computer is acting as client.
- **Passive FTP**
  - **Allow Incoming:** Allow Passive FTP when this computer is acting as a server.
  - **Allow Outgoing:** Allow Passive FTP when this computer is acting as a client.

Generally speaking, Active FTP is more secure from the server point of view, and Passive FTP is more secure from the client point of view.

UDP

- **Enable UDP stateful inspection:** Check to enable stateful inspection of UDP traffic.

The UDP stateful mechanism drops unsolicited incoming UDP packets. For every outgoing UDP packet, the rule will update its UDP "stateful" table and will then only allow a UDP response if it occurs within 60 seconds of the request. If you wish to allow specific incoming UDP traffic, you will have to create a **Force Allow** rule. For example, if you are running a DNS server, you will have to create a **Force Allow** rule to allow incoming UDP packets to destination port 53.

Without stateful inspection of UDP traffic, an attacker could masquerade as a DNS server and send unsolicited UDP "replies" from source port 53 to computers behind a firewall.

- **Enable UDP stateful logging:** Checking this option will enable the logging of UDP stateful inspection events.

ICMP

- **Enable ICMP stateful inspection:** Check to enable stateful inspection of ICMP traffic.

The ICMP (pseudo-)stateful mechanism drops incoming unsolicited ICMP packets. For every outgoing ICMP packet, the rule will create or update its ICMP "stateful" table and will then only allow a ICMP response if it occurs within 60 seconds of the request. (ICMP pair types supported: Type 0 & 8, 13 & 14, 15 & 16, 17 & 18.)

© Copyright 2011 Trend Micro Inc.
All rights reserved.

With stateful ICMP inspection enabled, you can, for example, only allow an ICMP echo-reply in if an echo-request has been sent out. Unrequested echo-replies could be a sign of several kinds of attack including a Smurf amplification attack, a Tribe Flood Network communication between master and daemon, or a Loki 2 back-door.

- **Enable ICMP stateful logging:** Checking this option will enable the logging of ICMP stateful inspection events.

Assigned To

The **Assigned To** tab lists the Security Profiles and computers that are making use of this stateful inspection configuration.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Deep Packet Inspection

Deep Packet Inspection

Turn DPI on or off and set the Inline DPI behavior to "Prevent" or "Detect".

When first applying a new set of DPI Rules you can choose to set the DPI behavior to "Detect". When in Detect mode, the DPI engine will apply all the same DPI Rules to traffic but instead of dropping packets, it will only log an Event and let the traffic pass. Use this behavior to ensure the new DPI Rules will not interfere with legitimate traffic.

This setting only applies when the Network Engine is operating **Inline**; that is, live traffic is being streamed through the Deep Security network engine. The alternative to Inline mode is Tap mode, where the live traffic is cloned, and it is only this cloned traffic that is analyzed by the network engine. Prevent mode is impossible when in Tap mode because the network engine does not control the live traffic stream.

To switch between Inline and Tap mode, go to **System > System Settings > Firewall and DPI**.

Recommendations

Agents can be configured to perform regular Recommendation Scans which scan a computer and make recommendations about the application of various Security Rules. Selecting this checkbox will automatically assign recommended rules for the computer and automatically unassign rules that are not required.

If you select this option, you should also opt to allow Deep Security Rule Updates to automatically assign new DPI Rules. Go to **System > System Settings > Updates** and select **Allow Deep Security Rule Updates to automatically assign new DPI Rules** in the **Deep Security Rule Updates** area.

To perform periodic Recommendation Scans , go to **System > System Settings > Scan**.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

DPI Events

By default, the Deep Security Manager collects Firewall and DPI Event logs from the Deep Security Agents/Appliances at every heartbeat. (This can be turned off from the **Firewall and DPI** tab in the **System > System Settings** screen.) The data from the logs is used to populate the various reports, graphs, and charts in the Deep Security Manager.

Once collected by the Deep Security Manager, Event logs are kept for a period of time which can be set from **System** tab in the **System > System Settings** screen. The default setting is one week.

From the main screen you can:

- **View** ( ) the properties of a particular event
- **Filter the list:** Use the **Period** and **Computer** toolbars to filter the list of events
- **Export** ( ) the event log data to a CSV file
- **Search** ( ) for a particular event

Additionally, right-clicking a log entry gives you the option to:

- **Add Tag(s):** Add an Event Tag to this event (See Event Tagging in the **Reference** section.)
- **Remove Tag(s):** Remove exiting event Tags
- **Computer Details:** View the Details screen of the computer that generated the log entry
- **DPI Rule Properties:** View the all the properties of a particular log entry on open **Properties** window
- **Whois Source IP:** Perform a whois on the source IP
- **Whois Destination IP:** Perform a whois on the destination IP

Columns for the DPI Events display:

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Reason:** The DPI Rule associated with this event.
- **Application Type:** The Application Type associated with the DPI Rule which caused this event.
- **Action:** What action the DPI Rule took (Allow, Deny, Force Allow, Log Only, or Detect Only (if the rule is in **Detect Only** mode)).
- **Rank:** The Ranking system provides a way to quantify the importance of DPI and Firewall Events. By assigning "asset values" to computers, and assigning "severity values" to DPI Rules and Firewall Rules, the importance ("Rank") of an Event is calculated by multiplying the two values together. This allows you to sort Events by Rank when viewing DPI or Firewall Events.
- **Direction:** The direction of the packet (incoming or outgoing)
- **Interface:** The MAC address of the interface through which the packet was passing.
- **Protocol:** Possible values are "ICMP", "IGMP", "GGP", "TCP", "PUP", "UDP", "IDP", "ND", "RAW", "TCP+UDP", AND "Other: nnn" where nnn represents a three digit decimal value.
- **Flags:** Flags set in the packet.
- **Source IP:** The packet's source IP.
- **Source MAC:** The packet's source MAC address.
- **Source Port:** The packet's source port.
- **Destination IP:** The packet's destination IP address.
- **Destination MAC:** The packet's destination MAC address.
- **Destination Port:** The packet's destination port.
- **Packet Size:** The size of the packet in bytes.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

View Event Properties

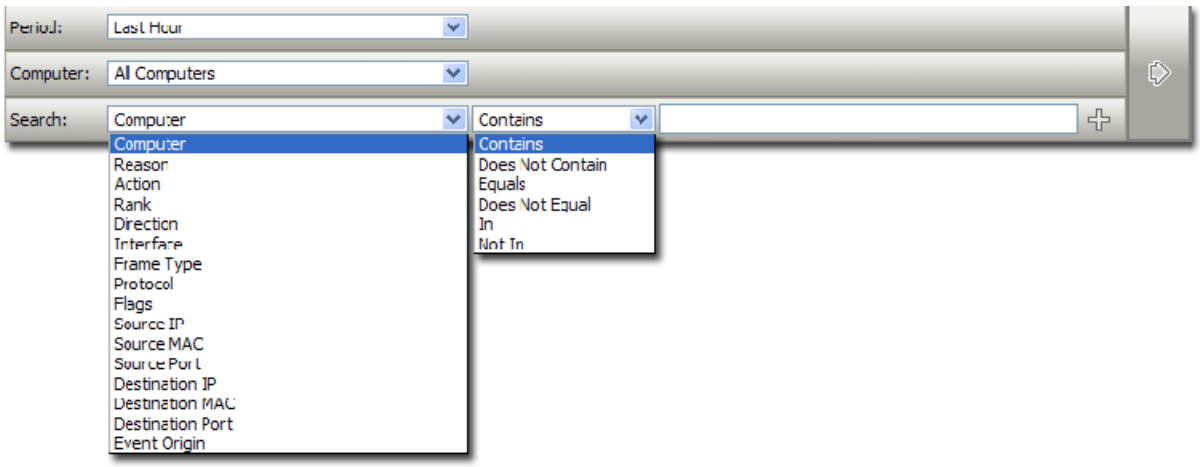
Double-clicking an event displays the **Properties** window for that entry. The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **System > System Settings > Tags**, and Event Tagging in the **Reference** section.

Filter the List and/or Search for an Event

Selecting "Open Advanced Search" from the "Advanced Search" drop-down menu toggles the display of the advanced search options.

The **Period** toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The **Computers** toolbar lets you organize the display of event log entries by computer groups or computer Security Profiles.



Advanced Search functions (searches are not case sensitive):

- **Contains:** The entry in the selected column contains the search string
- **Does Not Contain:** The entry in the selected column does not contain the search string
- **Equals:** The entry in the selected column exactly matches the search string
- **Does Not Equal:** The entry in the selected column does not exactly match the search string
- **In:** The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In:** The entry in the selected column does not exactly match any of the comma-separated search string entries

Pressing the "plus" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the submit button (at the right of the toolbars with the right-arrow on it).

Export...

Clicking the **Export...** button exports all event log entries to a CSV file.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

DPI Rules

Whereas Firewall Rules and Stateful Configurations examine a packet's control information (data that describes the packet), DPI Rules examine the actual content of the packet (and sequences of packets). Based on the conditions set within the DPI Rule, various actions are then carried out on these packets: from replacing specifically defined or suspicious byte sequences, to completely dropping packets and resetting the connection.

DPI Rule icons:

- Normal DPI Rules
- DPI Rules that operate according to a schedule
- DPI Rules that have configuration options
- DPI Rules that *require* configuration

The **DPI Rules** screen lets you create and manage DPI Rules. From the toolbar or the right-click shortcut menu you can:

- Create **New** DPI Rules from scratch (New)
- **Import** ( ) DPI Rules from an XML file
- Examine or modify the **Properties** of an existing DPI Rule ( )
- **Duplicate** (and then modify) existing DPI Rules ( )
- **Delete** a DPI Rule ( )
- **Export** ( ) one or more DPI Rules to an XML file. (Either export them all by click the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking **New** (New) or **Properties** ( ) displays the **DPI Rule Properties** window.

Note the **Configuration** tab. DPI Rules from Trend Micro are not directly editable through Deep Security Manager. Instead, if the DPI Rule requires (or allows) configuration, those configuration options will be available on the **Configuration** tab. Custom DPI Rules that you write yourself will be editable, in which case the **Rules** tab will be visible.

DPI Rule Properties

General Information

- **Name:** The name of the DPI Rule.
- **Description:** The description of the DPI Rule.
- **Minimum Agent/Appliance Version:** The minimum version of the Deep Security Agent/Appliance required to implement this DPI Rule.

Details

- **Application Type:** The Application Type this DPI Rule will be grouped under. You can select an existing type, or create a new one.

You can also edit existing types from this panel. Remember that if you edit an existing Application Type from here, the changes will be applied to all security elements making use of it.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **Priority:** The priority level of the DPI Rule. Higher priority rules are applied before lower priority rules.
- **Severity:** Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as a sorting criteria when viewing a list of DPI Rules. More importantly, each severity level is associated with a severity value; this value is multiplied by a computer's Asset Value to determine the Ranking of an Event. (See **System > System Settings > Ranking.**)
- **CVSS Score:** A measure of the severity of the vulnerability according the National Vulnerability Database.
- **Detect Only:** Use this checkbox when testing new rules. By checking this box, the rule will create a log entry prefaced with the words "detect only:" but will not interfere with traffic. If you set the "disable logging" checkbox in the next panel (below), the rule's activity will not be logged regardless of whether "Detect Only" is checked or not.

Some DPI Rules are designed to only operate in "Detect Only" mode and cannot be configured to block traffic. For theses rules, the "Detect Only" option will be set and locked so it cannot be changed.

Events

- **Disable Logging:** Check to disable Event logging.
  - **Generate Event on Packet Drop:** Log the dropping/blocking of a packet.
  - **Generate Event on Packet Modify:** Log the modification of a packet (i.e. if you are replacing a suspicious string of bytes.)
  - **Always Include Packet Data:** Includes the packet data in the log entry.
  - **Enable Debug Mode:** Logs multiple packets preceding and following the packet that triggered the rule. Trend Micro recommends only using this option if instructed to do so by your support provider.

Identification (Displayed for downloaded rules only)

- **Type:** Can be either Smart (one or more known and unknown (zero day) vulnerabilities), Exploit (a specific exploit, usually signature based), or Vulnerability (a specific vulnerability for which one or more exploits may exist).
- **Issued:** The date the Rule was released (not downloaded).
- **Identifier:** The rule's unique identifier tag.

Vulnerability (Displayed for Trend Micro rules only)

Displays information about this particular vulnerability. When applicable, the Common Vulnerability Scoring System (CVSS) is displayed. (For information on this scoring system, see the CVSS page at the National Vulnerability Database.)

Configuration (Displayed for Trend Micro rules only)

- **Configuration Options:** If the downloaded rule has any configurable options, they will be displayed here. Examples of options might be header length, allowed extensions for http, cookie length, etc. If you apply a rule without setting a required option, an alert will be triggered telling you which rule on which computer(s) requires configuration. (This also applies to any rules that are downloaded and automatically applied by way of a Security Update.)

DPI Rules that have configuration options are displayed in the **DPI Rules** screen with a small checkmark over their icon ( ).

© Copyright 2011 Trend Micro Inc.
All rights reserved.

View Rules (Available for custom DPI Rules only)

The **View Rules...** button will be available for DPI Rules that have not been marked confidential by Trend Micro. (Please contact Trend Micro for information on writing your own DPI Rules.)

Options

Alert

Select whether or not this DPI Rule should trigger an alert when it is triggered. If you only wish this rule to be active during specific periods, assign a schedule from the drop-down list.

Schedule

Select whether the DPI Rule should only be active during a scheduled time.

DPI Rules that are active only at scheduled times are displayed in the **DPI Rules** screen with a small clock over their icon ( ).

Context

Contexts are a powerful way of implementing different security policies depending on the computer's network environment. You will most often use Contexts to create Security Profiles which apply different Firewall and DPI Rules to computers (usually mobile laptops) depending on whether that computer is in or away from the office.

Contexts are designed to be associated with Firewall and DPI Rules. If the conditions defined in the Context associated with a Rule are met, the Rule is applied.

To determine a computer's location, Contexts examine the nature of the computer's connection to its domain controller. For more information on Contexts, see **Components > Contexts**.

Recommendation Options

Use this option to exclude this DPI Rule from Rule recommendations made after Recommendation Scans.

Assigned To

This tab displays the list of computers and Security Profiles to which this DPI Rule is assigned.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Application Types

The applications defined by Application Types are identified by the direction of traffic, the protocol being used, and the port through which the traffic passes. Application Types are a useful way of grouping DPI Rules. They are used to organize DPI Rules with a common purpose into groups. This simplifies the process of selecting a set of DPI Rules to assign to a computer. For example, consider the set of DPI Rules required to protect HTTP traffic to an Oracle Report Server. By grouping DPI Rules into Application Types it is easy to select rules in the "Web Server Common" and "Web Server Oracle Report Server" sets while excluding, for example, the set of rules that are specific to IIS Servers.

Application Type icons:

- Normal Application Types
- Application Types that have configuration options

From the main screen you can:

1. Define a **New** ( ) Application Type
2. View or edit the **Properties** ( ) of an existing Application Type
3. **Duplicate** (and then modify) existing Application Types ( )
4. **Delete** ( ) an Application Type

Clicking **New** (New) or **Properties** ( ) displays the Application Type **Properties** window.

General

General Information

The name and description of the Application Type. "Minimum Agent/Appliance Version" tells you what version of the Deep Security Agent/Appliance is required to support this Application Type.

Connection

- **Direction:** The direction of the initiating communication. That is, the direction of the first packet that establishes a connection between two computers. For example, if you wanted to define an Application Type for Web browsers, you would select "Outgoing" because it is the Web browser that sends the first packet to a server to establish a connection (even though you may only want to examine traffic traveling from the server to the browser). The DPI Rules associated with a particular Application Type can be written to examine individual packets traveling in either direction.
- **Protocol:** The protocol this Application Type applies to.
- **Port:** The port(s) this Application Type monitors. (*Not* the port(s) over which traffic is exclusively allowed.)

Configuration

The **Configuration** tab displays options that control how DPI Rules associated with this Application Type behave. For example, the "Web Server Common" Application Type has an option to "Monitor responses from Web Server". If this option is deselected, DPI Rules associated with this Application Type will not inspect response traffic over source port 80.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Options

Items in the **Options** tab control how the Deep Security Manager uses and applies the Application Type. For example, most Application Types have an option to exclude them from Recommendation Scans. This means that if the "Exclude from Recommendations" options is selected, a Recommendation Scan will not recommend this Application Type and its associated DPI Rules for a computer even if the application in question is detected.

Assigned To

The **Assigned To** tab lists the DPI Rules associated with this Application Type.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Integrity Monitoring

Integrity Monitoring allows you to monitor specific elements on a computer for changes. Deep Security has the ability to monitor installed software, running services, processes, files, directories, listening ports, registry keys, and registry values. It functions by performing a baseline scan of the elements on the computer specified in the assigned rules and then periodically rescanning those elements to look for changes. The Deep Security Manager ships with predefined Integrity Monitoring Rules and new Integrity Monitoring Rules are provided in Security Updates.

Recommendation Scans will recommend Integrity Monitoring Rules for a computer.

The typical procedure for enabling Integrity Monitoring on a computer is to:

1. Turn on Integrity Monitoring (either globally or on a specific computer)
2. Run a Recommendation Scan on the computer
3. Apply the recommended Integrity Monitoring Rules
4. Optionally, apply any Integrity Monitoring Rules you may have written yourself for the computer
5. Build a Baseline for the computer by opening the computer's **Details** window, going to the **Integrity Monitoring** screen, and clicking "Rebuild Baseline".
6. Periodically scan for changes (either manually or by creating a Scheduled Task)

Use the main **Integrity Monitoring** screen to turn Integrity Monitoring on or off and to set whether Integrity Monitoring Rules that are recommended after a Recommendation Scan are automatically applied.

- **Real Time:** Real Time Integrity Monitoring. Real Time Integrity Monitoring provides the ability to monitor Entity changes in real time and raise Integrity Monitoring events when changes are detected. Events are forwarded in real time via syslog to the SIEM or when the next heartbeat communication (configurable) to the Deep Security Manager occurs.
- **On:** Scheduled Integrity Monitoring Scans. Integrity Monitoring scans for changes can be scheduled just like other Deep Security operations, any changes to the Entities monitored since the last scan will be identified and an event raised. Note: multiple changes to the Entities being monitored in between scans will not be tracked, only the last change will be detected. To detect and report multiple changes to the Entities state being monitored, consider increasing the frequency of scheduled scans (i.e. daily instead of weekly for example) or select Real Time Integrity Monitoring for the Entities that change frequently.
- **Off:** On Demand Integrity Monitoring Scans. Integrity Monitoring scans for changes can also be initiated by the Administrator and would function similar to scheduled Integrity Monitoring scans.

Remember that these settings can be overridden at the Security Profile level or locally at the computer level. To do so, go to the Integrity screen on either the Security Profiles **Details** window or the computer's **Details** window.

The **Integrity Monitoring** screen in a computer's **Details** window has extra options that apply to the specific computer only. On it you can initiate a scan for changes or rebuild the baseline data for the computer. You can also initiate a Recommendation Scan or clear existing Recommendations.

For information on writing custom Integrity Monitoring Rules, see the documentation for the **Integrity Monitoring Rules** screen and Integrity Monitoring Rules Language in the **Reference** section.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Integrity Monitoring Events

Deep Security Manager collects Integrity Monitoring Events from the Deep Security Agents at every heartbeat. The data from the logs is used to populate the various reports, graphs, and charts in the Deep Security Manager.

Once collected by the Deep Security Manager, Event logs are kept for a period of time which can be set from **System** tab in the **System > System Settings** screen. The default setting is one week.

From the main screen you can:

- **View** ( ) the properties of a particular event
- **Filter the list:** Use the **Period** and **Computer** toolbars to filter the list of events
- **Export** ( ) the event list data to a CSV file
- **Search** ( ) for a particular event

Additionally, right-clicking a log entry gives you the option to:

- **Add Tag(s):** Add an Event Tag to this event (See Event Tagging in the **Reference** section.)
- **Remove Tag(s):** Remove exiting event Tags
- **Computer Details:** View the Details screen of the computer that generated the log entry
- **Integrity Monitoring Rule Properties:** View the properties of the Integrity Monitoring Rule associated with this event

View Event Properties

Double-clicking an event displays the **Properties** window for that entry which displays all the information about the event on one screen. The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **System > System Settings > Tags**, and Event Tagging in the **Reference** section.

Filter the List and/or Search for an Event

The **Period** toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The **Computers** toolbar lets you organize the display of event log entries by computer groups or computer Security Profiles.

Use the "Search" or "Advanced Search" options to search, sort, or filter displayed events.

Advanced Search functions (searches are not case sensitive):

- **Contains:** The entry in the selected column contains the search string
- **Does Not Contain:** The entry in the selected column does not contain the search string
- **Equals:** The entry in the selected column exactly matches the search string
- **Does Not Equal:** The entry in the selected column does not exactly match the search string
- **In:** The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In:** The entry in the selected column does not exactly match any of the comma-separated search string entries

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Export…

Clicking the **Export...** button exports all or selected events to a CSV file.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Integrity Monitoring Rules

Integrity Monitoring Rules allow the Deep Security Agents to scan for and detect changes to a computer's files, directories, and registry keys and values, as well as changes in installed software, processes, listening ports, and running services. These changes are logged as Events in the Manager and can be configured to generate alerts like any other Events. Integrity Monitoring Rules can be assigned directly to computers or can be made part of a Security Profile.

Integrity Monitoring Rules specify which Entities (files, registry keys, services, etc) to monitor for changes. Deep Security scans all the Entities specified by the rules assigned to a computer and creates a baseline against which to compare future scans of the computer. If future scans do not match the baseline, the Deep Security Manager will log an Integrity Monitoring Event and trigger an Alert (if so configured).

Integrity Monitoring Rule icons:

- Normal Integrity Monitoring Rules
- Integrity Monitoring Rules that operate according to a schedule
- Integrity Monitoring Rules that have configuration options
- Integrity Monitoring Rules that have configuration options and that operate according to a schedule

From the main screen you can:

- Create **New** Integrity Monitoring Rules from scratch (New)
- **Import** ( ) Integrity Monitoring Rules from an XML file
- Examine or modify the **Properties** of an existing Integrity Monitoring Rule ( )
- **Duplicate** (and then modify) existing Integrity Monitoring Rules ( )
- **Delete** a Integrity Monitoring Rule ( )
- **Export** ( ) one or more Integrity Monitoring Rules to an XML file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Integrity Monitoring Rules that are assigned to one or more computers or that are part of a Security Profile cannot be deleted.

Clicking **New** (New) or Properties ( ) displays the **Integrity Monitoring Rules Properties** window.

Integrity Monitoring Rule Properties

General Information

The name and description of the Integrity Monitoring Rule, and -- if the rule is issued by Trend Micro -- the minimum versions of the Agent and the Deep Security Manager that are required for the Rule to function.

Details

Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as a sorting criteria when viewing a list of Integrity Monitoring Rules. More importantly, each severity level is associated with a severity value; this value is multiplied by a computer's Asset Value to determine the Ranking of an Event. (See **System > System Settings > Ranking.**)

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Content

Note that the **Content** tab only appears for Integrity Monitoring Rules that you create yourself. Integrity Monitoring Rules issued by Trend Micro have a **Configuration** tab instead that displays the Integrity Monitoring Rule's configuration options (if any). Integrity Monitoring Rules issued by Trend Micro are not editable (although you can duplicate them and then edit the copy.)

You have the choice between three templates for creating new Integrity Rules: the **Registry Value** template, the **File** template, or the **Custom (XML)** template. Use the **Registry Value** template for creating Integrity Monitoring Rules that monitor changes to registry values. Use the **File** template for creating simple Integrity Monitoring Rules that monitor changes to files only. Use the **Custom (XML)** template to write rules in XML for monitoring directories, registry values, registry keys, services, processes, installed software, ports, (and files).

This section of the help describes the use of the **Registry Value** and **File** templates. For information on writing Integrity Monitoring Rules in XML using the Custom (XML) template, see Integrity Monitoring Rule Language in the **Reference** section.

Registry Value Template

Base Key

Select the base key to monitor and whether or not to monitor contents of sub keys.

Value Names

List value names to be included or excluded. Use "?" and "*" as wildcard characters.

Attributes

Use "Standard" to monitor changes in size or content. For other attributes, see *RegistryValueSet* in the **Reference** section under Integrity Rules Language.

File Template

Base Directory

Specifies the base directory for the rule. Everything else about the rule will be relative to this directory. Select "Include Sub Directories" to include sub directories. For example, a valid entry would be `C:\Program Files\MySQL` and selecting "Include Sub Directories".

File Names

Use the **File Names** fields to include or exclude specific files. Use wildcards ("?" for a single character and "*" for zero or more characters).

These fields can be left blank to monitor all files in the base directory, but this can be very demanding on system resources if there are many and/or large files in the directory.

Attributes

© Copyright 2011 Trend Micro Inc.
All rights reserved.

The following file attributes can be monitored for change:

- **Created:** Timestamp when the file was created.
- **LastModified:** Timestamp when the file was last modified.
- **LastAccessed:** Timestamp when the file was last accessed. On Windows this value does not get updated immediately, and recording of the last accessed timestamp can be disabled as a performance enhancement. See File Times for details. The act of scanning a file requires that the Agent open the file, which will change its last accessed timestamp. On Unix, the Agent will use the O_NOATIME flag if it is available when opening the file, which will prevent the OS from updating the last accessed timestamp and will speed up scanning.
- **Permissions:** The file's security descriptor (in SDDL format) on Windows or Posix-style ACLs on Unix systems that support ACLs, otherwise the Unix style rwxrwxrwx file permissions in numeric (octal) format.
- **Owner:** User ID of the file owner (commonly referred to as the "UID" on Unix).
- **Group:** Group ID of the file owner (commonly referred to as the "GID" on Unix).
- **Size:** size of the file.
- **Sha1:** SHA-1 hash.
- **Sha256:** SHA-256 hash.
- **Md5:** MD5 hash.
- **Flags:** Windows-only. Flags returned by the GetFileAttributes() Win32 API. Windows Explorer calls these the "Attributes" of the file: Readonly, Archived, Compressed, etc.
- **SymLinkPath** (Unix only): If the file is a symbolic link, the path of the link is stored here. Windows NTFS supports Unix-like symlinks, but only for directories, not files. Windows shortcut objects are not true symlinks since they are not handled by the OS; the Windows Explorer handles shortcut files (`*.lnk`) but other applications that open a `*.lnk` file will simply see the contents of the lnk file.
- **InodeNumber** (Unix only): The inode number of the file.
- **DeviceNumber** (Unix only): Device number of the disk on which the inode associated with the file is stored.
- **BlocksAllocated** (Unix only: The number of blocks allocated to store the file.

You can use the shorthand keyword "STANDARD", which will look for changes to:

- **Created**
- **LastModified**
- **Permissions**
- **Owner**
- **Group**
- **Size**
- **Contents**
- **Flags (Windows only)**
- **SymLinkPath (Unix only)**

Options

Triggers an Alert if the rule is triggered.

Assigned To

Displays a list of Security Profiles which include this Integrity Monitoring Rule as well as any computers to which this Integrity Monitoring Rule has been assigned directly. Integrity Monitoring Rules can be assigned to Security Profiles in the **Security Profiles** screen and to computers in the **Computers** screen.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Log Inspection

Log Inspection

The OSSEC Log Inspection Engine is integrated into Deep Security Deep Security Agents (6.0+) and gives Deep Security the ability to inspect the logs and events generated by the operating system and applications running on the computer. Log Inspection Rules can be assigned directly to computers or can be made part of a Security Profile. Like Integrity Monitoring Events, Log Inspection events can be configured to generate alerts in the Deep Security Manager.

Use the main Log Inspection screen to turn Log Inspection on or off.

Recommendations

Agents can be configured to perform regular Recommendation Scans which scan a computer and make recommendations about the application of various Security Rules. Selecting this checkbox will automatically assign recommended Log Inspection Rules to the computer and automatically unassign rules that are not required.

To turn the recommendation engine on or off, go to **System > System Settings > Scan**.

More Information

For more information on Log Inspection, see Options for Log Inspection Rules and Creating Custom Log Inspection Rules in the **Reference** section.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Log Inspection Events

Deep Security Manager collects Log Inspection Events from the Deep Security Agents at every heartbeat. The data from the logs is used to populate the various reports, graphs, and charts in the Deep Security Manager.

Once collected by the Deep Security Manager, Event logs are kept for a period of time which can be set from **System** tab in the **System > System Settings** screen. The default setting is one week.

From the main screen you can:

1. **View** ( ) the properties of a particular event
2. **Search** ( ) for a particular event
3. **Filter the list:** Use the **Period** and **Computer** toolbars to filter the list of events
4. **Export** ( ) the event list data to a CSV file

Additionally, right-clicking a log entry gives you the option to:

- **Add Tag(s):** Add an Event Tag to this event (See Event Tagging in the **Reference** section.)
- **Remove Tag(s):** Remove exiting event Tags
- **Computer Details:** View the Details screen of the computer that generated the log entry
- **Log Inspection Rule Properties:** View the properties of the Log Inspection Rule associated with this event

View Event Properties

Double-clicking an event displays the **Properties** window for that entry which displays all the information about the event on one screen. The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **System > System Settings > Tags**, and Event Tagging in the **Reference** section.

Filter the List and/or Search for an Event

The **Period** toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The **Computers** toolbar lets you organize the display of event log entries by computer groups or computer Security Profiles.

Use the "Search" or "Advanced Search" options to search, sort, or filter displayed events.

Advanced Search functions (searches are not case sensitive):

- **Contains:** The entry in the selected column contains the search string
- **Does Not Contain:** The entry in the selected column does not contain the search string
- **Equals:** The entry in the selected column exactly matches the search string
- **Does Not Equal:** The entry in the selected column does not exactly match the search string
- **In:** The entry in the selected column exactly matches one of the comma-separated search string entries
- **Not In:** The entry in the selected column does not exactly match any of the comma-separated search string entries

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Export…

Clicking the **Export...** button exports all event log entries to a CSV file.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Log Inspection Rules

The Deep Security Log Inspection module provides you the ability to collect and analyze operating system and application logs optimized to identify important security events buried in 1000's of log entries. These events can be sent to a security information and event management (SIEM) system, or centralized logging server for correlation, reporting, and archiving. All events are also securely collected centrally at Deep Security Manager.

This article describes the properties and configuration options of existing Log Inspection Rules provided by Trend Micro. For information on creating new custom Log Inspection Rules, see Creating Custom Log Inspection Rules in the **Reference** section.

Deep Security Manager ships with a standard set of OSSEC Log Inspection Rules. For information on writing your own Log Inspection Rules using the XML-based language, consult the OSSEC documentation or contact your support provider.

This help article describes the properties of a new "Basic" Log Inspection Rule. For an explanation of the **Configuration** tab options of the predefined OSSEC Log Inspection Rules, see Options for Log Inspection Rules in the **Reference** section.

To write a new Log Inspection Rule using the "Basic" interface, click **New** In the Log Inspection toolbar to display the **New Log Inspection Rule Properties** window.

General

Type the name and a description for your new rule.

Content

Template

In the **Content** tab, select the "Basic Rule" template.

General Information

Enter a Rule ID. A Rule ID is a unique identifier for the rule. OSSEC defines 100000 - 109999 as the space for User-defined rules. (Deep Security Manager will pre-populate the field with a new unique Rule ID.)

Give the rule a level. Zero (0) means the rule never logs an event, although other rules that watch for this rule may fire. (See the dependency fields below.)

Optionally assign the rule to one or more comma-separated groups. This can come into play when dependency is used since you can create rules that fire on the firing of a rule, or a rule that belongs to a specific group.

Pattern Matching

This is the pattern the rule will look for in the logs. The rule will be triggered on a match. Pattern matching supports Regular Expressions or simpler String Patterns. The "String Pattern" pattern type is faster than RegEx but it only supports three special operations:

- **^ (caret)**: specifies the beginning of text

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **$ (dollar sign)**: specifies the end of text
- **| (pipe)**: to create a "OR" between multiple patterns

Composite

Frequency is the number of times the rule has to match within a specific time frame before the rule is triggered.

Time Frame is the period of time in seconds within which the rule has to trigger a certain number of times (the frequency, above) to log an event.

Dependency

Setting a dependency on another rule will cause your rule to only log an event if the rule specified in this area has also triggered.

Files

Type the full path to the file(s) you want your rule to monitor and specify the type of file it is.

Options

Alert

Select whether this rule triggers an alert in the Deep Security Manager or not.

The "Alert Minimum Severity" setting is only used if you have written "multiple rules" within your rule -- something that cannot be done using the "Basic" template. However, if after creating your rule using the "Basic' template, you edit the XML of the rule and add additional rules to the XML which have different severity levels, you can use the "Alert Minimum Severity Level" drop-down menu to set the minimum severity from the multiple rules which will trigger an Alert.

Assigned To

Lists which Security Profiles or computers are using this Log Inspection Rule.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Log Inspection Decoders

The Log Inspection Rules included with Deep Security Manager require "1002791 - Default Decoders" to function. Users should not have to write their own decoders.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Components

Directory Lists

Reusable lists of Directories.

File Lists

Reusable lists of Files.

File Extension Lists

Reusable lists of File Extensions.

IP Lists

Reusable lists of IPs.

MAC Lists

Reusable lists of MAC addresses.

Port Lists

Reusable lists of ports.

Contexts

Contexts which specify the circumstances under which a Firewall or DPI Rule is in effect.

Schedules

Reusable schedules.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Directory Lists

The Directory Lists component contains a list of all directories that are assigned by the Anti-Malware configuration page. Use the **Directory Lists** section to create reusable lists of valid directories.

From the main screen you can:

- Create a **New Directory List** ( ) from scratch
- **Import from File** ( ) imports scan directory lists from an XML file
- Examine or modify the **Properties** of an existing directory list ( )
- **Duplicate** (and then modify) existing directory lists ( )
- **Delete** a directory list ( )
- **Export** ( ) one or more directory list(s) to an XML file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)
- **Add/Remove Columns** ( ) columns can be added or removed by clicking **Add/Remove Columns**. The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Clicking **New** (New) or **Properties** ( ) displays the Directory List **Properties** window.

Directory List Properties

General Information

The name and description of the directory list.

Directory(ies)

Type the directory(ies) that are going to be on your list. Only put one directory per line.

Supported Formats

Directory Example: `c:\program files\`

You can also insert comments into your directory list by preceding the text with a pound sign ("#"), such as Directory #Comment

Example: `c:\testdirectory # Exclude`

Assigned To

The **Assigned To** tab lists the rules making use of this directory list. Clicking the names of the rules displays their **Properties** window.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

File Lists

The File Lists component contains list of files that are assigned by the Anti-Malware configuration page under the **Exclusion** tab.

General

Each file is assigned per line and stored in the "ScanFileLists" table. Use the **File Lists** section to create a reusable lists of valid files. From the main screen you can:

- Create a **New File List** ( ) from scratch
- **Import from File** ( ) imports scan files from an XML file
- Examine or modify the **Properties** of an existing file list ( )
- **Duplicate** (and then modify) existing file lists ( )
- **Delete** a file list ( )
- **Export** ( ) one or more file list(s) to an XML file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)
- **Add/Remove Columns** ( ) columns can be added or removed by clicking **Add/Remove Columns**. The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Clicking **New** (New) or **Properties** ( ) displays the File List **Properties** window.

File List Properties

General Information

The name and description of the file list.

File(s)

Type the file(s) that are going to be on your list. Only put one filename per line.

Supported Formats

Filename Example: testfile.doc

You can also insert comments into your file list by preceding the text with a pound sign ("#"), such as File #Comment

Example: c:\folder\file.txt #

Assigned To

The **Assigned To** tab lists the names of the files making use of this file list. Clicking the names of the file lists displays their **Properties** windows.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

File Extension Lists

The **File Extension Lists** screen contains a list of file extensions that are used by **Anti-Malware Configurations**. For example, one list of file extensions can be used by multiple Anti-Malware Configurations as files to include in a scan. Another list of file extensions can be used by multiple Anti-Malware Configurations as files to exclude from a scan.

From the main screen you can:

- Create a **New File Extension List** ( ) from scratch
- **Import from File** ( ) imports scan file extensions from an XML file
- Examine or modify the **Properties** of an existing file extension list ( )
- **Duplicate** (and then modify) existing file extension lists ( )
- **Delete** a file extension list ( )
- **Export** ( ) one or more file extension list(s) to an XML file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)
- **Add/Remove Columns** ( ) columns can be added or removed by clicking **Add/Remove Columns**. The order in which the columns are displayed can be controlled by dragging them into their new position. Listed items can be sorted and searched by the contents of any column.

Clicking **New** (New) or **Properties** ( ) displays the File Extension Lists **Properties** window.

File Extension List Properties

General Information

The name and description of the file extension list.

File Extensions(s)

Type the file extension(s) that are going to be on your list. Only put one extension per line.

Assigned To

The **Assigned To** tab lists the rules making use of this file extension list. Clicking the names of the rules displays their **Properties** window.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

IP Lists

Use the **IP Lists** screen to create reusable lists of IP addresses for use by multiple Firewall Rules. From the main screen you can:

- Create **New** IP Lists from scratch (New)
- **Import** ( ) IP Lists from an XML file
- Examine or modify the **Properties** of an existing IP List ( )
- **Duplicate** (and then modify) existing IP Lists ( )
- **Delete** an IP List ( )
- **Export** ( ) one or more IP lists to an XML file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking **New** (New) or Properties ( ) displays the IP List **Properties** window.

IP List Properties

General Information

The name and description of the IP list.

IPs

Type the IP addresses, masked IP addresses, and IP address ranges that are going to be on your list. Only put one of these per line.

Supported Formats

As well as individual addresses, you can enter IP ranges and masked IPs. Use these examples to properly format your entries. (You can insert comments into your IP list by preceding the text with a hash sign ("#").)

Assigned To

The **Assigned To** tab lists the rules making use of this IP List. Clicking the names of the rules displays their **Properties** window.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

MAC Lists

Use the **MAC Lists** section to create reusable lists of MAC addresses.
From the main screen you can:

- Create **New** ( ) MAC lists from scratch
- **Import** ( ) MAC lists from an XML file
- Examine or modify the **Properties** of an existing MAC list ( )
- **Duplicate** (and then modify) existing MAC lists ( )
- **Delete** a MAC list ( )
- **Export** ( ) one or more MAC lists to an XML file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking **New** (New) or Properties ( ) displays the MAC List **Properties** window.

MAC List Properties

General Information

The name and description of the list.

MAC(s)

Type the MAC addresses that are going to be on your list. Only put one of these per line.

Supported Formats

The MAC(s) list supports MAC addresses in both hyphen- and colon-separated formats. Use these examples to properly format your entries. (You can insert comments into your MAC list by preceding the text with a pound sign ("#").)

Assigned To

The **Assigned To** tab lists the rules making use of this MAC list. Clicking the names of the rules displays their **Properties** window.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Port Lists

Use the **Port Lists** screen to create reusable lists of ports.
From the main screen you can:

- Create **New** port lists from scratch (New)
- **Import** ( ) port lists from an XML file
- Examine or modify the **Properties** of an existing port list ( )
- **Duplicate** (and then modify) existing port lists ( )
- **Delete** a port list ( )
- **Export** ( ) one or more port lists to an XML file. (Either export them all by click the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking **New** (New) or **Properties** ( ) displays the Port List **properties window.**

Port List Properties

General Information

The name and description of the list.

Port(s)

Enter the ports that are going to be on your list. Only put one of these per line.

For a listing of which ports are used for what, see the Internet Assigned Numbers Authority (IANA)

Supported Formats

Individual ports and port ranges can be included on the list. Use these examples to properly format your entries. (You can insert comments into your port list by preceding the text with a pound sign ("#").)

Assigned To

The **Assigned To** tab lists the rules making use of this port list. Clicking the names of the rules displays their **Properties** window.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Contexts

Contexts are a powerful way of implementing different security policies depending on the computer's network environment.

Contexts are designed to be associated with Firewall and DPI Rules. If the conditions defined in the Context associated with a Rule are met, the Rule is applied. (To link a Security Rule to a Context, go to the **Options** tab in the Security Rule's **Properties** window and select the Context from the "Context" drop-down menu.)

Contexts can be used to provide Agents with "location awareness". To determine a computer's location, Contexts examine the nature of the computer's connection to its domain controller and connectivity to the internet. Select the "Context applies when Domain Controller connection is: " option and choose from the following:

- **Locally Connected to Domain:** true only if the computer can connect to its domain controller directly
- **Remotely Connected to Domain:** true if the computer can only connect to its domain controller via VPN
- **Not Connected to Domain:** true if the computer cannot connect to its domain controller by any means
- **Not Connected to Domain, No Internet Connectivity:** true if the computer cannot connect to its domain controller by any means and the host has no Internet connectivity. (The test for Internet connectivity can be configured in **System > System Settings > Contexts**.)

By assessing the ability of the computer to connect with its domain controller or the Internet, the Agent can then implement rules such as restricting HTTP traffic to non-routable ("private") IP addresses only.

For an example of a Security Profile that implements Firewall Rules using Contexts, examine the properties of the "Location Aware - High" Security Profile.

From the toolbar or the right-click shortcut menu on the **Contexts** screen, you can:

- Create **New** (New) Contexts from scratch
- **Import** ( ) Contexts from an XML file
- Examine or modify the **Properties** of an existing Context ( )
- **Duplicate** (and then modify) existing Contexts ( )
- **Delete** a Context ( )
- **Export** ( ) one or more Contexts to an XML file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking **New** (New) or Properties( ) displays the Context **Properties** window.

Context Properties

General Information

The name and description of the Context Rule as well as the earliest version of the Deep Security Agent the rule is compatible with.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Options

Context applies when Domain Controller connection is

Specifying an option here will determine whether or not the Firewall Rule is in effect depending on the ability of the computer to connect to its Domain Controller or its Internet Connectivity. (Conditions for testing Internet Connectivity can be configured in **System > System Settings > Contexts**.)

If the Domain Controller can be contacted directly (via ICMP), the connection is "Local". If it can be contacted via VPN only, then the connection is "Remote (VPN) ".

The time interval between Domain Controller connectivity test is the same as the Internet Connectivity Test interval which is also configurable in **System > System Settings > Contexts**.

The Internet Connectivity Test is only performed if the computer is unable to connect to its Domain Controller.

Context Applies to Interface Isolation Restricted Interfaces

This context will apply to network interfaces on which traffic has been restricted through the use of Interface Isolation. (Primarily used for Allow or Force Allow Firewall Rules.)

Assigned To

The **Assigned To** tab displays a list of the rules making use of this Context.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Schedules

Schedules are rule components used to define when a particular Firewall or DPI rule is in effect. Schedules can also be used to specify when the Manager can communicate with Agents/Appliances to update a Security Profile.

Note that other non-rule based Scheduled Tasks such as downloading and applying new Security Updates can be defined from **System > Tasks**.

From the toolbar or the right-click shortcut menu you can:

- Create **New** schedules from scratch (New)
- **Import** ( ) schedules from an XML file
- Examine or modify the **Properties** of an existing schedule ( )
- **Duplicate** (and then modify) existing schedules ( )
- **Delete** a schedule ( )
- **Export** ( ) one or more schedules to an XML file. (Either export them all by clicking the **Export...** button, or choose from the drop-down list to export only those that are selected or displayed)

Clicking New (New) or Properties ( ) displays the Schedule properties window.

Schedule Properties

Schedule periods are defined by hour-long time blocks. Clicking a time block selects it, and shift-clicking de-selects it.

Assigned To

The **Assigned To** tab displays a list of the rules making use of this schedule.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

System

System Events

Use the System Events screen to examine system-related events (as opposed to security-related events).

System Settings

The Settings section lets you control the administration of the Deep Security system.

System Information

The System Information screen contains details about the current state of the Deep Security Manager.

Tags

All currently defined tags are displayed in the Tags screen.

Tasks

The Tasks section provides the ability to configure recurring automated and event-based tasks.

Roles

Use the Roles section to define various roles with different rights. Roles are then assigned to Users.

Users

Use the Users section to create and modify User accounts for Users of the Deep Security Manager.

Contacts

Use the Contacts section to create and modify contacts.

License

The license page displays details about your Trend Micro product license such as which Deep Security Modules are available and how many computers you are licensed to install Agent/Appliance software on.

Updates

The Updates section allows you to manage security and software updates.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

System Events

The System Event log is a record of system-related events (as opposed to security-related events). From the main screen you can:

1. **View** ( ) the details (properties) of a system event
2. **Search** ( ) for a particular system event
3. **Export** ( ) currently displayed system events to a CSV file

Additionally, right-clicking a log entry gives you the option to:

- **Add Tag(s):** Add an Event Tag to this event (See Event Tagging in the **Reference** section.)
- **Remove Tag(s):** Remove exiting Event Tags

View

Selecting an event and clicking **View** ( ) displays the **Event Viewer Properties** window.

General

General Information

- **Time:** The time according to the system clock on the computer hosting the Deep Security Manager.
- **Level:** The severity level of event that occurred. Event levels include **Info**, **Warning**, and **Error**.
- **Event ID:** The event type's unique identifier.
- **Event:** The name of the event (associated with the event ID.)
- **Target:** The system object associated with the event will be identified here. Clicking the object's identification will display the object's properties sheet.
- **Action Performed By:** If the event was initiated by a User, that User's username will be displayed here. Clicking the username will display the **User Properties** window.
- **Manager:** The hostname of the Deep Security Manager computer.

Description

If appropriate, the specific details of what action was performed to trigger this entry in the system event log will be displayed here.

Tags

The **Tags** tab displays tags that have been attached to this Event. For More information on Event tagging, see **System > System Settings > Tags**, and Event Tagging in the **Reference** section.

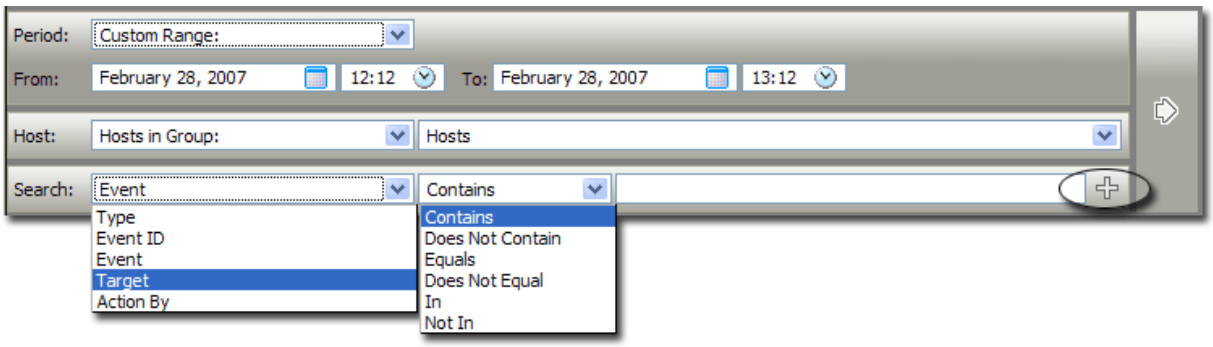
Filter the List and/or Search for an Event

The **Period** toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

The **Computers** toolbar lets you organize the display of event log entries by computer groups or computer Security Profiles.

Clicking **Advanced Search** toggles the display of the search bar.



Pressing the "Add Search Bar" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the "Submit Request" button (at the right of the toolbars with the right-arrow on it).

Export

You can export displayed events to a CSV file. (Paging is ignored, all pages will be exported.) You have the option of displaying the displayed list or the selected items.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

System Settings

The **System > System Settings** screen lets you control the administration of the Deep Security system. This section is for managing system configuration settings such as session timeouts, system alerts, communications between Agents/Appliances and the Manager, heartbeat settings, etc.

Note that the **Settings** screen has a **Save** button at the bottom right. Changes made to these settings (all tabs) must be saved before they take effect.

- Computers
- Anti-Malware
- Firewall and DPI
- Integrity Monitoring
- Log Inspection
- Interface Isolation
- Contexts
- Reconnaissance
- Scan
- Notifications
- Ranking
- System Events
- Security
- Updates
- System

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Computers

Communication Direction

- **Bidirectional:** By default, communications are bi-directional. This means that the Agent/Appliance normally initiates the heartbeat but still listens on the Agent port for Manager connections. The Manager is still free to contact the Agent/Appliance in order to perform operations as required. This allows the Manager to apply changes to the security configuration to the Agent/Appliance as they occur.
- **Manager Initiated:** With this option selected, all Manager to Agent/Appliance communications are initiated by the Manager. This includes security configuration updates, heartbeat operations, and requests for Event logs.
- **Agent/Appliance Initiated:** With this option selected, the Agent/Appliance does not listen on port 4118. Instead it contacts the Manager on the heartbeat port (4120 by default) as dictated by the heartbeat settings. Once the Agent/Appliance has established a TCP connection with the Manager all normal communication takes place: the Manager first asks the Agent/Appliance for its status and for any events. (This is the heartbeat operation). If there are outstanding operations that need to be performed on the computer (e.g., the Security Profile needs to be updated), these operations are performed before the connection is closed. In this mode, communications between the Manager and the Agent/Appliance only occur on every heartbeat. If an Agent/Appliance's security configuration has changed, it will not be updated until the next heartbeat.

Before configuring an Agent/Appliance for Agent/Appliance initiated communication, ensure that the Manager URL and heartbeat port can be reached by the Agent/Appliance. If the Agent/Appliance is unable to resolve the Manager URL or is unable to reach the IP and port, Agent/Appliance initiated communications will fail for this Agent/Appliance. The Manager URL and the heartbeat port are listed in the **System Details** area in the **System > System Information** screen.

Note that Agents/Appliances look for the Deep Security Manager on the network by the Manager's hostname. Therefore the Manager's hostname **must** be in your local DNS for Agent/Appliance initiated or bidirectional communication to work.

To enable communications between the Manager and the Agents/Appliances, the Manager automatically implements a (hidden) Firewall Rule (priority four, Bypass) which opens port 4118 on the Agents/Appliances to incoming TCP/IP traffic. The default settings open the port to any IP address and any MAC address. You can restrict incoming traffic on this port by creating a new priority 4, Force Allow or Bypass Firewall Rule, which only allows incoming TCP/IP traffic from specific IP and/or MAC addresses. This new Firewall Rule will replace the hidden Firewall Rule if the settings match the following:

action: force allow or bypass
priority: 4 - highest
packet's direction: incoming
frame type: IP
protocol: TCP
packet's destination port: 4118 (or a list or range that includes 4118)

As long as these settings are in effect, the new rule will replace the hidden rule. You can then type Packet Source information for IP and/or MAC addresses to restrict traffic to the computer.

Hostnames

Update the "Hostname" entry if an IP is used as a hostname and a change in IP is detected on the computer after Agent/Appliance-initiated communication or discovery: Turn this option on if, for example, your network has no DNS and you are using dynamic IPs. (Deep Security Manager always identifies computers/Agents/Appliances by their unique fingerprint, not their IP addresses.)

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Remote Activation

The default process of installing and activating an Agent on a computer is as follows: the Agent is installed on a computer and then a User uses the Deep Security Manager to "activate the Agent". This activation sends a unique encrypted fingerprint from the Manager to the Agent. The Agent now knows not to accept any instructions not identified as coming from the Manager by that fingerprint. There may be circumstances, however, where it is desirable for the activation to be initiated by the Agent rather than by the Manager. (Large, distributed installations, for example.) In this case the Manager must be configured to allow Agents to communicate with it and initiate activation. Use the **Remote Activation** panel to set restrictions on which computers can initiate their own Agent activations.

Agent initiated activation is performed from the command-line. The following are the Agent's activation-related command-line options:

Usage: `dsa_control [/a <str>] [/g <str>] [/c <str>] [/r]`		**Notes**
`/a <str>`	**Activate** Agent with DSM at specified URL. URL format must be "dsm://hostOrIp:port/"	"port" is the Manager's Heartbeat port. (4120 by default.)
`/g <str>`	**Agent** URL. Defaults to "https://127.0.0.1:4118/"	
`/c <str>`	**Certificate** file	
`/r`	**Reset** Agent configuration	

You can instruct Deep Security Manager to send a default Security Profile to self-activating Agents which do not already have a Security Profile assigned to them. Use the **Security Profile to assign (when no Security Profile is currently assigned)** to select a Security Profile.

Heartbeat

- **Heartbeat Interval (in minutes):** How much time passes between heartbeats.
- **Number of Heartbeats that can be missed before an alert is raised :** Several missed heartbeats in a row may indicate a problem with the Agent/Appliance or the computer. This setting determines how many missed heartbeats are allowed to go by before the Manager triggers an alert. (For example, entering three will cause the Manager to trigger an alert on the fourth missed heartbeat.)
- **Maximum change (in minutes) of the local system time on the computer between heartbeats before an alert is raised:** For Agents that are capable of detecting changes to the system clock (Windows Agents) these events are reported to the Manager as Agent Event 5004. If the change exceeds the clock change listed here then an alert is triggered. For Agents that do not support this capability (non-Windows Agents), the Manager monitors the system time reported by the Agent at each heartbeat operation and will trigger an alert if it detects a change greater than the permissible change specified in this setting.

Once a **Computer-Clock-Changed** alert is triggered, it must be dismissed manually.

- **Raise Offline Errors For Inactive Virtual Machines:** Sets whether an Offline error is raised if the virtual machine is stopped or paused.

Automatically Update Computers

By default, any time you make a change to any element in the Deep Security system, all affected computers are immediately updated. For example, if you edit a port list, all computers already making use of that port list will get updated immediately. (If you make such a change and then look at the **Computers** screen, you will see the updates happening.) Not setting the **Automatically update all affected**

© Copyright 2011 Trend Micro Inc.
All rights reserved.

computers after changing any aspect of the Deep Security System option means that after any changes, you will have to find affected computers on the **Computers** screen, right-click them and choose "Update Agent(s) Now" from the context menu.

Note that this applies to Security Updates as well. If a Security Update includes, for example, an updated port list for Oracle servers, the updated port list will be deployed to all computers currently making use of that port list unless you have selected the manual option.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Anti-Malware

Smart Scan

Smart Scan is a technology which can shorten the interval between Anti-Malware pattern updates while at the same time reducing the traffic load on your network caused by the distribution of pattern updates to your Deep Security Virtual Appliances.

When Smart Scan is enabled, instead of downloading a complete pattern file from ActiveUpdate servers, a Smart Scan server delivers a highly compressed *Smart Scan Agent Pattern* file to your Virtual Appliances. This pattern file is used to identify suspicious files on endpoint computers. When a suspicious file is identified, a fingerprint of the file is sent to a local Smart Scan server for analysis by the more rigorous *Smart Scan Pattern* which is updated on an hourly basis.

When Smart Scan is not enabled, complete Anti-Malware pattern files are downloaded to your Virtual Appliances from the conventional ActiveUpdate servers.

Smart Scan Server

If you have enabled Smart Scan you must enter the URL of at least one locally installed Smart Scan server. Smart Scan server software along with installation and configuration instructions are available from the Trend Micro Download Center at http://downloadcenter.trendmicro.com.

Deep Security 7.5 currently only supports Smart Scan server 1.x. Version 2.0 of the software has since been released and been renamed "Smart Protection Server". To download version 1.x, go to the Smart Protection Server download page and click on "View other versions".

Note that you can enter the addresses of several Smart Scan servers. Trend Micro recommends that you install multiple local servers to ensure availability in case of hardware, software, or connectivity failure.

Quarantined Files

- **Maximum disk utilization for storing quarantined file:** The maximum space allocated on the Virtual Appliance for storing all quarantined files.
- **Maximum disk utilization for a guest VM:** The maximum space allocated on the Virtual Appliance for storing the quarantined files from an individual VM.
- **Maximum quarantined file size:** The maximum size allowed on the Virtual Appliance for an individual quarantined file.

If any of these maximums is exceeded when the Virtual Appliance tries to retrieve a quarantined file, the operation will fail and an alert will be raised.

Quarantined files will be automatically deleted from a Virtual Appliance under the following circumstances:

- If a VM undergoes vMotion, quarantined files associated with that VM will be deleted from the Virtual Appliance.
- If a VM is deactivated from the Deep Security Manager, quarantined files associated with that VM will be deleted from the Virtual Appliance.
- If a Virtual Appliance is deactivated from the Deep Security Manager, all the quarantined files stored on that Virtual Appliance will be deleted.
- If a Virtual Appliance is deleted from the vCenter, all the quarantined files stored on that Virtual Appliance will also be deleted.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Firewall and DPI

Network Engine Mode

The Agent/Appliance's network engine can operate Inline or in Tap Mode. When operating Inline, the live packet stream passes through the network engine. Stateful tables are maintained, Firewall Rules are applied and traffic normalization is carried out so that DPI Rules can be applied to payload content. When operating in Tap Mode, the live packet stream is cloned and diverted from the main stream. In Tap Mode, the live packet stream is not modified; all operations are carried out on the cloned stream.

Events

You can set the maximum size of each individual log file and how many of the most recent files are kept. Event log files will be written to until they reach the maximum allowed size, at which point a new file will be created and written to until it reaches the maximum size and so on. Once the maximum number of files is reached, the oldest will be deleted before a new file is created. Event log entries usually average around 200 bytes in size and so a 4MB log file will hold about 20,000 log entries. How quickly your log files fill up depends on the number of rules in place.

- **Maximum size of the event log files (on Agent/Appliance):** Adjust these settings if you begin to see "Insufficient Disk Space" alerts for one or more computers.
- **Number of event log files to retain (on Agent/Appliance):** Adjust these settings if you begin to see "Insufficient Disk Space" alerts for one or more computers.
- **Collect Firewall Events from Agent/Appliance:** Retrieve the latest Firewall Events from the Agent/Appliance at every Heartbeat.
- **Collect DPI Events from Agent/Appliance:** Retrieve the latest DPI Events from the Agent/Appliance at every Heartbeat.

Events are records of individual events. **Counters** are a record of the number of times individual events have occurred. Events are used to populate the **Events** screens. Counters are used to populate the Dashboard Widgets (number of Firewall Events over the last 7 days, etc.) and the Reports. You might want to collect only counters if, for example, you are using syslog for event collection; events can potentially take up a lot of disk space and you may not want to store the data twice.

- **Do Not Record Events with Source IP of:** This option is useful if you want Deep Security to not make record Events for traffic from certain trusted computers.

The following three settings let you fine tune Event aggregation. To save disk space, Deep Security Agents/Appliances will take multiple occurrences of identical events and aggregate them into a single entry and append a "repeat count", a "first occurrence" timestamp, and a "last occurrence" timestamp. To aggregate event entries, Deep Security Agents/Appliances need to cache the entries in memory while they are being aggregated before writing them to disk.

- **Cache Size:** Determines how many types of events to track at any given time. Setting a value of 10 means that 10 types of events will be tracked (with a repeat count, first occurrence timestamp, and last occurrence timestamp). When a new type of event occurs, the oldest of the 10 aggregated events will be flushed from the cache and written to disk.
- **Cache Lifetime:** Determines how long to keep a record in the cache before flushing it to disk. If this value is 10 minutes and nothing else causes the record to be flushed, any record that reaches an age of 10 minutes gets flushed to disk.
- **Cache Staletime:** Determines how long to keep a record whose repeat count has not been recently incremented. If Cache Lifetime is 10 minutes and Cache Staletime is two minutes, an event record which has gone two minutes without being incremented will be flushed and written to disk.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Regardless of the above settings, the cache is flushed whenever Events are sent to the Deep Security Manager.

- **Generate Firewall Events for packets that are "Out Of Allowed Policy":**Select whether you wish to log packets that are dropped because they have not been specifically permitted by an **Allow** rule or Firewall Rule. (Note that turning this option on can significantly increase the size of your log files.
- **Allow DPI Rules to capture data for the first hit of each rule (in period):** Keep the data from the packet that triggered a log entry. (The packet's data can be viewed with the log entry. Each rule will only capture data once in a five second period to avoid unduly large log files.)

Advanced

Use Custom Driver Settings

- **CLOSED timeout:** For gateway use. When a gateway passes on a "hard close" (RST), the side of the gateway that received the RST will keep the connection alive for this amount of time before closing it.
- **SYN_SENT Timeout:** How long to stay in the SYN-SENT state before closing the connection.
- **SYN_RCVD Timeout:** How long to stay in the SYN_RCVD state before closing the connection.
- **FIN_WAIT1 Timeout:** How long to stay in the FIN-WAIT1 state before closing the connection.
- **ESTABLISHED Timeout:** How long to stay in the ESTABLISHED state before closing the connection.
- **ERROR Timeout:** How long to maintain a connection in an Error state. (For UDP connections, the error can be caused by any of a variety of UDP problems. For TCP connections, the errors are probably due to packets being dropped by the firewall.)
- **DISCONNECT Timeout:** How long to maintain idle connections before disconnecting.
- **CLOSE_WAIT Timeout:** How long to stay in the CLOSE-WAIT state before closing the connection.
- **CLOSING Timeout:** How long to stay in the CLOSING state before closing the connection.
- **LAST_ACK Timeout:** How long to stay in the LAST-ACK state before closing the connection.
- **ACK Storm timeout:** The maximum period of time between retransmitted ACKs within an ACK Storm. In other words, if ACKs are being retransmitted at a lower frequency then this timeout, they will NOT be considered part of an ACK Storm.
- **Boot Start Timeout:** For gateway use. When a gateway is booted, there may already exist established connections passing through the gateway. This timeout defines the amount of time to allow non-SYN packets that could be part of a connection that was established before the gateway was booted to close.
- **Cold Start Timeout:** Amount of time to allow non-SYN packets that could belong to a connection that was established before the stateful mechanism was started.
- **UDP Timeout:** Maximum duration of a UDP connection.
- **ICMP Timeout:** Maximum duration of an ICMP connection.
- **Allow Null IP:** Allow or block packets with no source and/or destination IP address.
- **Block IPv6:** Block or Allow IPv6 packets. (DPI Filtering of IPv6 traffic is not supported. It can only be blocked or allowed.)
- **Connection Cleanup Timeout:** Time between cleanup of closed connections (see next).
- **Maximum Connections per Cleanup:** Maximum number of closed connections to cleanup per periodic connection cleanup (see previous).
- **Block Same Src-Dest IP Address:** Block or allow packets with same source and destination IP address. (Doesn't apply to loopback interface.)
- **Maximum TCP Connections:** Maximum simultaneous TCP Connections.
- **Maximum UDP Connections:** Maximum simultaneous UDP Connections.
- **Maximum ICMP Connections:** Maximum simultaneous ICMP Connections.
- **Maximum Events per Second:** Maximum number of events that can be written per second.
- **TCP MSS Limit:** The MSS is the Maximum Segment Size (or largest amount of data) that can be sent in a TCP packet without being fragmented. This is usually established when two computers establish communication. However, in some occasions, the traffic goes through a router or switch that has a smaller MSS. In this case the MSS can change. This causes retransmission of the packets and the Agent/Appliance logs them as "Dropped Retransmit". In cases where there are

© Copyright 2011 Trend Micro Inc.
All rights reserved.

large numbers of Dropped Retransmit event entries, you may wish to lower this limit and see if the volume is reduced.

- **Number of Event Nodes:** The maximum amount of kernel memory the driver will use to store log/event information for folding at any one time.

Event folding occurs when many Events of the same type occur in succession. In such cases, the Agent/Appliance will "fold" all the events into one.

- **Ignore Status Code:** This option lets you ignore certain types of Events. If, for example, you are getting a lot of "Invalid Flags" you can simply ignore all instances of that Event.
- **Ignore Status Code:** Same as above.
- **Ignore Status Code:** Same as above.
- **Advanced Logging Policy:**
  - **Bypass:** No filtering of Events. Overrides the "Ignore Status Code" settings (above) and other advanced settings, but does not override logging settings defined in the Deep Security Manager. For example, if Stateful Configuration logging options set from a Stateful Configuration Properties window in the Deep Security Manager will not be affected.
  - **Default:** Will switch to "Tap Mode" (below) if the engine is in Tap Mode, and will switch to "Normal" (above) if the engine is in Inline Mode. **Normal:** All Events are logged except dropped retransmits.
  - **Backwards Compatibility Mode:** For support use only.
  - **Verbose Mode:** Same as "Normal" but including dropped retransmits.
  - **Stateful and Normalization Suppression:** Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, unsolicited udp, unsolicited ICMP, out of allowed policy.
  - **Stateful, Normalization, and Frag Suppression:** Ignores everything that "**Stateful and Normalization Suppression**" ignores as well as events related to fragmentation.
  - **Stateful, Frag, and Verifier Suppression:** Ignores everything "**Stateful, Normalization, and Frag Suppression**" ignores as well as verifier-related events.
  - **Tap Mode:** Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, max ack retransmit, packet on closed connection.

For a more comprehensive list of which Events are ignored in **Stateful and Normalization Suppression; Stateful, Normalization, and Frag Suppression; Stateful, Frag, and Verifier Suppression; and Tap** modes, see Advanced Logging Policy Modes in the **Reference** section.

- **Silent TCP Connection Drop:** When Silent TCP Connection Drop is on, a RST packet is only sent to the local stack. No RST packet is sent on the wire. This reduces the amount of information sent back to a potential attacker.

If you enable the Silent TCP Connection Drop you must also adjust the DISCONNECT Timeout. Possible values for DISCONNECT Timeout range from 0 seconds to 10 minutes. This must be set high enough that the connection is closed by the application before it is closed by the Deep Security Agent/Appliance. Factors that will affect the DISCONNECT Timeout value include the operating system, the applications that are creating the connections, and network topology.

- **Enable Debug Mode:** When in debug mode, the Agent/Appliance captures a certain number of packets (specified by the setting below: Number of Packets to retain in Debug Mode). When a rule is triggered and debug mode is on, the Agent/Appliance will keep a record of the last X packets that passed before the rule was triggered. It will return those packets to the Manager as Debug Events.

Note that debug mode can very easily cause excessive log generation and should only be used under Client Services supervision.

- **Number of Packets to retain in Debug Mode:** The number of packets to retain and log when debug mode is on.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **Log All Packet Data:** All internally defined logs (ie: not FW/DPI/verifier) which have not been aggregated will attach the full packet data to their log. This and the following two settings are equivalent to the matching DPI and FW log settings.
- **Log only one packet within period:** If the above is not set, but this is set, then most logs will only contain the header data with a full packet being attached only periodically.
- **Period for Log only one packet within period:** The period between when full packet data will be logged if the above is set.
- **Maximum data size to store when packet data is captured:** The maximum size of header or packet data to be attached to a log.
- **Standby Mode Pulse Interval:** When appliance protection is used in conjunction with an in-guest Agent a heartbeat is sent with this period to ensure the in-guest Agent is working.
- **Standby Mode Pulse Timeout:** When the appliance is in standby mode and the in-guest Agent is stopped, then after this number of heartbeat intervals are missed the appliance takes over network protection.
- **Standby Mode Stable Timeout:** After detecting that the in-guest Agent is functioning for this number of heartbeat intervals, the appliance switches back to standby mode.
- **Generate Connection Events for TCP:** Generates a Firewall Event every time a TCP connection is established.
- **Generate Connection Events for ICMP:** Generates a Firewall Event every time an ICMP connection is established.
- **Generate Connection Events for UDP:** Generates a Firewall Event every time a UDP connection is established.
- **Bypass CISCO WAAS Connections:** This mode bypasses stateful analysis of TCP sequence numbers for connections initiated with the proprietary CISCO WAAS TCP option selected. This protocol carries extra information in invalid TCP Sequence and ACK numbers that interfere with stateful firewall checks. Only enable this option if you are using CISCO WAAS and you are seeing connections with Invalid SEQ or Invalid ACK in the firewall logs. When this option is selected, TCP stateful sequence number checks are still performed for non WAAS enabled connections.
- **Drop Evasive Retransmit:** Incoming packets containing data that has already been processed will be dropped to avoid possible evasive retransmit attack techniques.
- **Verify TCP Checksum:** The segment's checksum field data will be used to assess the integrity of the segment.
- **Minimum Fragment Offset:** Defines the minimum acceptable IP fragment offset. Packets with offsets less than this will be dropped with reason "IP fragment offset too small". If set to 0 no limit is enforced. (default 60)
- **Minimum Fragment Size:** Defines the minimum acceptable IP fragment size. Fragmented packets that are smaller than this will be dropped with reason "First fragment too small" as potentially malicious. (default 120)
- **Fragment Timeout:** How long to keep fragmented packets.
- **Maximum number of fragmented IP packets to keep:** If configured to do so, the DPI Rules will edit the content of a packet (or packet fragment) if that content is considered suspicious. This setting determines how long after editing to wait for the remaining packet fragments before discarding the packet.
- **Send ICMP to indicate fragmented packet timeout exceeded:** Whether not to indicate to remote computer with an ICMP packet that a connection timeout has been exceeded

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Integrity Monitoring

Content Hash Algorithms

Select the hash algorithm(s) that will be used for integrity monitoring. You can select more than one algorithm, but this is not recommended because of the detrimental effect on performance.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Log Inspection

Severity Clipping

Send Agent/Appliance events to syslog when they equal or exceed the following severity level : Log Inspection Rules have a severity level. This setting determines which Events triggered by those rules get sent to the syslog server (if syslog is enabled.) (To enable syslog, go to **System > System Settings > Notifications**.)

Store events at the Agent/Appliance for later retrieval by DSM when they equal or exceed the following severity level : This setting determines which Log Inspection Events are kept in the database and displayed in the **Log Inspection Events** screen.

Tag Options

Automatically apply tags for the log inspection groups: LI rules have groups associated with them in the rules. For example:

```
<rule id="18126" level="3">
  <if_sid>18101</if_sid>
  <id>^20158</id>
  <description>Remote access login success</description>
  <group>authentication_success,</group>
</rule>

<rule id="18127" level="8">
  <if_sid>18104</if_sid>
  <id>^646|^647</id>
  <description>Computer account changed/deleted</description>
  <group>account_changed,</group>
</rule>
```

Each group name has a "friendly" name string associated with it. In the above example, "authentication_success" would be "Authentication Success", "account_changed" would be "Account Changed". When this checkbox is set, the friendly names are automatically added as a tag for that event. If multiple rules trigger, multiple tags will be attached to the event.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Interface Isolation

Interface Isolation

Interface Isolation allows you to force a computer to use only one interface at any one time. This feature was designed to prevent attackers from bridging across two interfaces.

Interface Patterns

To enforce interface isolation, set the **Enable Interface Isolation** option and enter string patterns that will match the names of the interfaces on a computer (in order of priority). You can use standard regular expression syntax when creating your list of interfaces.

Note that if you enter a string pattern that matches more than one interface on a computer, then traffic will be allowed on all of those matching interfaces. To make sure that only one interface is active, set the **Limit to one active interface** option.

This is an option you may not want to set at the global level, but at more granular levels for particular Security Profiles or computers only. To do this, set the global settings to *not* enforce interface isolation and then override the setting on the Security Profile or the computer. For more information on overriding settings, see Inheritance and Overrides in the **Reference** section.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Contexts

Use this screen to configure the settings Deep Security will use to determine whether a protected computer has Internet connectivity or not. Some Deep Security Rules can be applied conditionally depending on the computer's network connectivity conditions. This is known as "Location Awareness". The Internet connectivity condition options for a particular rule can be configured on the **Options** tab of the rule's **Properties** window. The Internet Connectivity Test can also be used when implementing Interface Isolation. (See **System > System Settings > Interface Isolation**.)

Internet Connectivity Test

- **URL for testing Internet Connectivity Status:** The URL to which an HTTP request will be sent to test Internet Connectivity. (You must include "http://".)
- **Regular Expression for returned content used to confirm Internet Connectivity Status:** A regular expression which will be applied to the returned content to confirm that HTTP communication was successful.
- **Test Interval:** The time interval between connectivity tests.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Reconnaissance

Reconnaissance Scans

The **Reconnaissance** screen allows Users to enable and configure traffic analysis settings on all or selected computers.

- **Reconnaissance Scan Detection Enabled:** Perform detection.
- **Computers/Networks on which to perform detection:** Choose from the drop-down list the IPs to protect. Choose from existing IP Lists. (You can use the **Components > IP Lists** screen to create an IP List specifically for this purpose.)
- **Do not perform detection on traffic coming from:** Select from a set of IP Lists which computers and networks to ignore. (As above, you can use the **Components > IP Lists** screen to create an IP List specifically for this purpose.)

For each type of attack, the Agent/Appliance can be instructed to send the information to the Deep Security Manager where an alert will be triggered. You can configure the Manager to send an email notification when the alerts are triggered. (See **System > System Settings > Notifications**. The Alerts are: "Network or Port Scan Detected", "Computer OS Fingerprint Probe Detected", "TCP Null Scan Detected", "TCP FIN Scan Detected", and "TCP Xmas Scan Detected.") Select **Notify DSM Immediately** for this option.

Stateful Inspection must be on and TCP and UDP Logging enabled for Reconnaissance protection to function. Stateful Inspection and logging can be enabled in the **Firewall > Stateful Configurations** screen.

Once an attack has been detected, you can instruct the Agents/Appliances to block traffic from the source IPs for a period of time. Use the **Block Traffic** drop-down lists to set the number of minutes.

- **Computer OS Fingerprint Probe:** The Agents/Appliances will recognize and react to active TCP stack OS fingerprinting attempts.
- **Network or Port Scan:** The Agents/Appliances will recognize and react to port scans.
- **TCP Null Scan:** The Agents/Appliances will refuse packets with no flags set.
- **TCP SYNFIN Scan:** The Agents/Appliances will refuse packets with only the SYN and FIN flags set.
- **TCP Xmas Scan:** The Agents/Appliances will refuse packets with only the FIN, URG, and PSH flags set or a value of 0xFF (every possible flag set).

"Computer OS Fingerprint Probe" and "Network or Port Scans" differ from the other three types of reconnaissance in that they cannot be recognized by a single packet.

The Agent/Appliance reports a computer or port scan if it detects that a remote IP is visiting an abnormal ratio of IPs to ports. Normally an Agent/Appliance computer will only see traffic destined for itself, so a port scan is by far the most common type of probe that will be detected. However, if a computer is acting as a router or bridge it could see traffic destined for a number of other computers, making it possible for the Agent/Appliance to detect a computer scan (ex. scanning a whole subnet for computers with port 80 open).

Detecting these scans can take several seconds since the Agent/Appliance needs to be able to track failed connections and decide that there are an abnormal number of failed connections coming from a single computer in a relatively short period of time.

The statistical analysis method used in computer/port scan detection is derived from the "TAPS" algorithm proposed in the paper "Connectionless Port Scan Detection on the Backbone" published by Sprint/Nextel and presented at the Malware workshop, held in conjunction with IPCCC, Phoenix, AZ, USA in April, 2006.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Deep Security Agents running on Windows computers with browser applications may occasionally report false-positive reconnaissance scans due to residual traffic arriving from closed connections.

For the "Notify DSM Immediately" option to work, the Agents/Appliances must be configured for **Agent/Appliance initiated** or **bi-directional** communication. (See **System > System Settings > Computers.**) If enabled, the Agent/Appliance will initiate a heartbeat to the Deep Security Manager immediately upon detecting the attack or probe.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Scan

Scanning for Open Ports

Select a port list to be used when the Deep Security Manager performs a port scan on discovered computers. (The port lists in the drop-down list are the same ones defined in the **Port Lists** screen in the **Components** section.)

Scanning for Recommendations

Periodically, the Agents can scan their computer for common applications and then make rule recommendations based on what is detected. This setting sets the interval between scans on computers that have been configured to allow them.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Notifications

Alert Notification (from the Manager)

Enter an email address to which all alert emails will be sent regardless of whether any Users have been set up to receive notifications. (Which alerts will trigger the sending of an email can be configured from the **System > System Settings > System** screen.)

Notification Frequency (From the Agent/Appliance)

Select how often events are sent from the Agent/Appliance to alert recipients. (Enter Syslog configuration below.)

Anti-Malware Event Notification (from the Agent/Appliance)

Forward Events to a Remote Computer (via Syslog)

If you wish to store your logs on a dedicated syslog server, type the required information in these fields. For information on configuring Syslog, see Configuring Syslog Integration.

Firewall and DPI Event Notification (from the Agent/Appliance)

Forward Events to a Remote Computer (via Syslog)

If you wish to store your logs on a dedicated syslog server, type the required information in these fields. For information on configuring Syslog, see Configuring Syslog Integration.

Integrity Monitoring Event Notification (from the Agent/Appliance)

Forward Events to a Remote Computer (via Syslog)

If you wish to store your logs on a dedicated syslog server, type the required information in these fields. For information on configuring Syslog, see Configuring Syslog Integration.

Log Inspection Event Notification (from the Agent/Appliance)

Forward Events to a Remote Computer (via Syslog)

If you wish to store your logs on a dedicated syslog server, type the required information in these fields. For information on configuring Syslog, see Configuring Syslog Integration.

System Event Notification (from the Manager)

Forward System Events to a Remote Computer (via Syslog)

Notifications can be sent to a Syslog server. Type the details of your syslog server here. For information on configuring Syslog, see Configuring Syslog Integration.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Forward System Events to a Remote Computer (via SNMP)

Deep Security also supports SNMP. The MIB file ("DeepSecurity.mib") is located in `\Trend Micro\Deep Security Manager\util`.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Ranking

Ranking

The Ranking system provides a way to quantify the importance of DPI and Firewall Events. By assigning "asset values" to computers, and assigning "severity values" to DPI Rules and Firewall Rules, the importance ("Rank") of an Event is calculated by multiplying the two values together. This allows you to sort Events by Rank when viewing DPI or Firewall Events.

Firewall Rule Severity Values

Severity values for Firewall Rules are linked to their actions: Deny, Log Only, and Packet Rejection. (The latter refers to packets rejected because of a stateful configuration setting.) Use this panel to edit the severity values which will be multiplied by a computer's asset value to determine the rank of a Firewall Event. (A Firewall Rule's actions can viewed and edited in the Rule's **Properties** window.)

DPI Rule Severity Values

DPI Rule Severity Values are linked to their severity levels: Critical, High, Medium, or Low. Use this panel to edit their values which will be multiplied by a computer's asset value to determine the rank of a DPI Event. A DPI Rule's severity setting can be viewed in the Rule's **Properties** window.

Integrity Monitoring Rule Severity Values

Integrity Monitoring Rule Severity Values are linked to their severity levels: Critical, High, Medium, or Low. Use this panel to edit their values which will be multiplied by a computer's asset value to determine the rank of an Integrity Monitoring Event. An Integrity Monitoring Rule's severity can be viewed in the Rule's **Properties** window.

Log Inspection Rule Severity Values

Log Inspection Rule Severity Values are linked to their severity levels: Critical, High, Medium, or Low. Use this panel to edit their values which will be multiplied by a computer's asset value to determine the rank of a Log Inspection Event. A Log Inspection Rule's severity level can be viewed and edited from the Rule's **Properties** window.

Asset Values

Asset Values are not associated with any of their other properties like DPI Rules or Firewall Rules. Instead, Asset Values are properties in themselves. A computer's Asset Value can be viewed and edited from the computer's **Details** window. To simplify the process of assigning asset values, you can predefine some values that will appear in the **Asset Importance** drop-down list in the first screen of the computer's **Details** window. To view existing predefined computer Asset Values, click the **View Asset Values...** button in this panel. The **Asset Values** window displays the predefined settings. These values can be changed, and new ones can be created. (New settings will appear in the drop-down list for all computers.)

© Copyright 2011 Trend Micro Inc.
All rights reserved.

System Events

System Events

"System Events" include changes to the configuration of an Agent/Appliance, the Deep Security Manager, or Users. They also include errors that may occur during normal operation of the Deep Security system. This screen is used to set whether particular events are recorded and whether email notifications should be sent if they occur.

For a list of all possible System Events, see **System Events** in the **Reference** section.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Security

Security

User Security

- **Session Timeout (min):** Specify the period of inactivity after which a User will be required to sign in again.
- **Incorrect Sign-In Attempts (Before Lock Out):**The number of times an individual User (i.e. with a specific username) can attempt to sign in with an incorrect password before he is locked out. Only a User with "Can Edit User Properties" rights can unlock a locked-out User.
- **User Password Minimum Length:** The minimum number of characters required in a password.
- **User Password Requires Both Letters and Numbers:** Letters (a-z, A-Z) as well as numbers (0-9) must be used as part of the password.
- **User Password Requires Both Upper and Lower Case Characters:** Upper and lower case characters must be used.
- **User Password Requires Non-Alphanumeric Characters:** Passwords must include non-alphanumeric characters.

For greater security, enforce stringent password requirements: minimum 8 characters, include both numbers and letters, use upper and lower case, include non-alphanumeric characters, and expire regularly.

A note about being signed in as two Users at once: Remember that Firefox sets session cookies on a per-process basis, and not on a per-window basis. This means that if for some reason you want to be signed in as two Users at the same time, you will either have to use two different browsers (if one of them is Firefox), or log in from two separate computers.

If a User gets locked out for a particular reason (too many failed login attempts, for example), and no User remains with the sufficient rights to unlock that account, please contact Trend Micro for assistance.

Sign In Page Message

You can optionally display a message on the Deep Security Manager's sign in page.

Trusted Certificates

View Certificate List: Click the **View Certificate List...** button to view al list of all security certificates accepted by Deep Security Manager.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Updates

To ensure maximum protection you must keep your pattern files, anti-malware engines, and software components current. The **Updates** tab on the **System > System Settings** screen allows you to set the location where Deep Security Manager checks for updates. To see the status of current updates, go to the **System > Updates** screen.

Download Updates From

You have three location options:

- **Trend Micro Active Update Server:** Connect to the default Trend Micro Update Server.
- **Other Update Source:** If you were given an alternative source for updates, enter the URL here (including "http://").
- **Intranet location containing a copy of the current file:** If you retrieve the update file separately and store it on another computer, enter the file's location here.

When entering the username, you must include the domain or hostname (or IP address), i.e. "domain\username" or "hostname\username".

Appliance Update Configuration

Select whether you want to automatically update Virtual Appliances with the latest rules, anti-malware patterns, and engines as they become available.

Proxy Settings for Updates and License Notifications

If you use a proxy server for updates and license notifications, enter the details here.

Deep Security Rule Updates

- **Allow Deep Security Rule Updates to automatically assign new DPI Rules:** New DPI Rules in Security Updates are associated with Application Types (HTTP Server, DNS Client, MS SQL Server, etc.). If this option is checked, new DPI Rules can automatically be assigned to computers on which the new DPI Rule's associated Application Type is active. Two conditions must be met for a rule to be automatically assigned to a computer:
    1. This option must be selected on this screen.
    2. The rule itself, created by Trend Micro, must be designed to allow auto-assignment. (Some rules, although associated with an Application Type, are not intended to be auto-assigned. The Deep Security Manager will recognize these rules and not apply them even if this option is checked.)
- **Allow Deep Security Rule Updates to set an alert on new DPI Rules:** Some new DPI Rules are considered important enough by Trend Micro that they are set to trigger an alert by default. Clearing this will override that default behavior.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

System

System

Alert Configuration

Configure all of Deep Security Manager's possible Alerts. For the most part, this means turning them on or off, setting their severity levels, and configuring the Alert's email notification settings.

SMTP

Type the address of your SMTP mail (with the port if required). Enter a "From" email address from which the emails should be sent. Optionally enter a "bounce" address to which delivery failure notifications should be sent if the alert emails can't be delivered to one or more Users. If your SMTP mail server requires outgoing authentication, enter the username and password credentials. Once you've entered the necessary information, use the **Test SMTP Settings** to test the settings.

Web Service API

Much of the Deep Security Manager's functionality can be controlled via SOAP-invoked Web services. The WSDL can be found at the URL displayed in the panel on the screen. For assistance with Deep Security Manager's Web services API, please contact Trend Micro.

Note that a Users ability to access Web Services in the Deep Security Manager will depend on that User being granted the appropriate privileges. These privileges are associated with the Role the User has been assigned. The setting is found on the **General** tab of the **Role properties window** found at **System > Roles**.

Prune

These settings define how long to store Event records and Counters, older Security Updates, and older versions of Agent/Appliance software before a purge removes them from the database.

With respect to the Event settings, your decisions should be based on the robustness of the database system you are using, the amount of available storage space, and which events you have decided to log. Some tips on logging:

- Disable log collection for computers that are not of interest. This can be done through the **Advanced Settings** in the computer **Details** window or the Security Profile **Details** window.
- Consider reducing the logging of Firewall Rule activity by disabling the logging options in the Stateful Configuration. (For example, disabling the UDP logging will eliminate the unsolicited UDP log entries)
- For DPI Rules the best practice is to log only dropped packets. Logging packet modifications may result in a lot of log entries.
- For DPI Rules, only include packet data (an option in the DPI Rule's **Properties** window) when you are interested in examining the source of attacks. Otherwise leaving packet data on will result in much larger log sizes.

Logs are used to populate the Events pages. **Counters** are data aggregated from the logs. They are used to generate Reports and populate the Dashboard widgets.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Export

The encoding used when you export data files from the Deep Security Manager.

WHOIS

The whois lookup to be used when logging DPI and Firewall Events.

Licenses

- **Hide Unlicensed Modules For New Users:** Determines whether unlicensed modules are hidden rather than simply grayed out for subsequently created Users. (This setting can be overridden on a per-User basis on the **System > Users > Properties** window).

© Copyright 2011 Trend Micro Inc.
All rights reserved.

System Information

Create a Diagnostic Package...

Clicking **Create Diagnostic Package...** in the Toolbar displays the **Diagnostic Package** wizard which will create a zip file containing Install/Uninstall and Debug Logs, System Information, Database Contents (last hour only for time-sensitive items), and a File Listing. This information can be given to your support provider to help troubleshoot any problems.

The default maximum size of a diagnostic package is approximately 200MB. A command line instruction is available to increase the size of the diagnostic package:

```
dsm_c -action changesetting -name
configuration.diagnosticMaximumFileSize -value ####
```

The following example increases the size of the package to 1GB (1000MB):

```
dsm_c -action changesetting -name
configuration.diagnosticMaximumFileSize -value 1000
```

Do not change the size of the diagnostic package unless instructed to do so by your support provider.

Managers...

Click on **Managers...** to display a list of all active Manager nodes. Double-click on a Manager in the list (or click on the graphical representation of a Manager node in the **Network Map with Activity Graph** in the **System Activity** panel) to display its **Properties** window:

- **Hostname:** The hostname of the Deep Security Manager host computer.
- **Description:** A description of the Manager node.
- **Performance:** A Deep Security Manager's performance can be affected by several factors including number of CPUs, available bandwidth, and database responsiveness. The Manager's default performance settings are designed to be suited for most installation environments. However, if you experience performance issues your support provider may suggest that you change the Performance Profile assigned to one or more of your Deep Security Manager nodes. (You should not change these settings without first consulting your support provider.)
  - **Aggressive:** This Performance Profile is optimized for installations where the Deep Security Manager is installed on a dedicated server. The following table gives an indication of how some common concurrent operations are distributed per Manager node using the **Aggressive** Performance Profile:

Operation	2-core system	8-core system
Activations	10	20
Updates	25	50
Recommendation Scans	5	12
Check Status	100	Same (100)
Agent/Appliance-Initiated Heartbeats	20 Active 40 Queued	50 Active 40 Queued

  - **Standard:** This Performance Profile is optimized for installations where the Deep Security Manager and the database share the same host. The following table gives an indication of how some common concurrent operations are distributed per Manager node using the **Standard** Performance Profile:

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Operation	2-core system	8-core system
Activations	5	10
Updates	16	46
Recommendation Scans	3	9
Check Status	65	100
Agent/Appliance-Initiated Heartbeats	20 Active 40 Queued	50 Active 40 Queued

- **None:** No optimization. The following table gives an indication of how some common concurrent operations are distributed per Manager node using no Performance Profile:

Operation	2-core system	8-core system
Activations	10	40
Updates	10	40
Recommendation Scans	10	40
Check Status	10	40
Agent/Appliance-Initiated Heartbeats	40 Active	160 Active

- **Status:** Indicates whether the Deep Security Manager node whose properties you are viewing is online and active from the perspective of the Deep Security Manager node you are logged into.
- **Options:** You can choose to decommission the Manager node. The node has to be offline (uninstalled or service halted) to be decommissioned.

For more information on multi-node Deep Security Manager installations, see Multi-Node Manager in the Reference section.

Extensions...

Extensions can be reports or plug-ins for the Deep Security Manager.

Demo Mode...

If you are evaluating Deep Security in a test environment and want to see what a full Deep Security installation in an enterprise environment looks like, you can enable Demo Mode by clicking **Demo Mode...** on the **System Information** screen toolbar.

When in Demo Mode, the Manager populates its database with simulated computers, Events, Alerts, and other data. Initially, seven days worth of data is generated but new data is generated on an ongoing basis to keep the Manager's Dashboard, Reports and Events screens populated with data.

While Demo Mode can be used with mixed real and simulated computers, it is **not** intended to be used in a production environment!

Demo mode can be turned off the same way.

About

This panel displays the version number of the Deep Security Manager node you are currently logged in to.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

System Activity (Over The Last Hour)

This panel displays various graphs detailing activities carried out by the different Manager nodes. For details on the information displayed in the **System Activity** panel, see Multi Node Manager in the Reference section.

System Details

This panel displays detailed system information used for troubleshooting by your support provider.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Tags

Event Tagging allows administrators to manually tag events with predefined labels ("attack", "suspicious", "patch", "acceptable change", "false positive", "high priority", etc.) and the ability to define custom labels ("Assigned to Tom for review", etc.).

In addition to the manual tagging of events, automated event tagging can be accomplished via the use of a "Reference Computer" which is particularly useful for managing Integrity Monitoring events. For example, a planned rollout of a patch can be applied to the reference computer, the events associated with the application of the patch can be tagged as "Patch X", similar events raised on other systems can automatically be deemed to be "acceptable changes" and suppressed to reduce the number of events subjected to scrutiny by an administrator.

Event tagging enables specialized views of events, dashboards, and reports and can be applied to a single event, similar events, or even to all future similar events.

Tags

All currently defined tags are displayed in the **System > Tags** screen. This includes predefined as well as custom tags. (Only tags that are currently in use are displayed.)

Delete Tags: Deleting a tag removes the tag from all events to which it is attached.

Auto-Tag Rules

Auto-Tag Rules are created by selecting events and choosing to tag similar items.

For information on Event Tagging procedures, see Event Tagging in the **Reference** section.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Tasks

The **Tasks** screen lets you automate and schedule certain common tasks. There are two kinds of Tasks: Scheduled Tasks and Event-based Tasks. Scheduled Tasks will initiate a procedure according to a defined schedule and Event-based Tasks will initiate a procedure when a particular Event occurs.

From the main screen you can:

- Create **New** Tasks (New)
- Examine or modify the **Properties** of an existing Task ( )
- **Duplicate** (and then modify) existing Tasks ( )
- **Delete** a Task ( )
- **Run** ( ) a selected Task (Scheduled Tasks only)

Click **New** ( ) and select either "New Scheduled Task" or "New Event-based Task" The wizard that appears will guide you through the steps of creating a new Task. You will be prompted for different information depending on the type of task.

Scheduled Tasks

The following Tasks can be scheduled:

- **Generate Report:** Automatically generate reports and optionally have them emailed to a list of Users.
- **Discover Computers:** Periodically check for new computers on the network by scheduling a Discovery operation. You will be prompted for an IP range to check and asked to specify which computer group the new computer will be added to.
- **Alert Summary:** Generate an email listing all outstanding (unresolved) alerts.
- **Run Script:** If the Syslog and SNMP options do not meet your event notification requirements, it may be possible for Trend Micro to provide a solution using custom-written scripts. Please contact Trend Micro for more information.
- **Scan Computers for Integrity Changes:** Causes the Deep Security Manager to perform an Integrity Scan to compare a computer's current state against its baseline.
- **Scan computers for Malware:** Schedules an Anti-Malware Scan. The configuration of the scan is the same as that specified on the **System > System Settings > Anti-Malware** screen for each computer.
- **Synchronize Directory:** Synchronize the Computers list with an added LDAP directory. (Only available if you have added an LDAP directory to the Deep Security Manager.)
- **Update Computers:** Periodically perform an update operation on selected computers. An update operation ensure that all configuration changes made in the Deep Security Manager have been applied.
- **Component Update:** Regularly check for security Updates and download and optionally install them if any are available.
- **Scan Computers for Recommendations:** Causes the Deep Security Manager to scan the computer(s) for common applications and then make recommendations based on what is detected.
- **Synchronize VMware vCenter:** Synchronize the **Computers** list with an added VMware vCenter. (Only available if you have added a VMware vCenter to the Deep Security Manager.)
- **Check for New Software:** Check if new versions of the Manager, Agents, Appliance or Filter Driver are available.
- **Scan Computers for Open Ports:** Schedule periodic port scans on one or more computers. You can specify individual computers or all computers belonging to a particular computer group. The ports that will be scanned are those defined on the **Scan** tab in the **System > System Settings** screen.
- **Backup:** Perform regular database backups. (This option is only available if you are using a Derby or Microsoft SQL Server database.)

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Event-based Tasks

This following events can be monitored:

- **Computer Created (by System):** A Computer being added to the Deep Security Manager during synchronization with an Active Directory, or the creation of a virtual machine on a managed ESX server running a Virtual Appliance.
- **Computer Moved (by System):** A virtual machine being moved from an unmanaged ESX Server to a managed ESX Server running a Virtual Appliance.

Conditions can be imposed on the events; use standard regular expression syntax to match patterns in the following fields:

- Computer name
- vCenter name
- ESX name
- Folder (and parent folders)
- Platform
- Whether Virtual Appliance protection is available

Depending on the source of the new computer, some fields may not be available. For example, "Platform" would not be available for computers added as a result of the synchronization with an Active Directory.

The following actions can be taken once any of the above events is detected:

- **Activate Computer:** The new Computer is automatically activated.
- **Assign Security Profile:** The new Computer is automatically assigned a Security Profile. (The Computer must be activated first.)

Activation will only occur if the computer is not already activated. That is, activation will only occur if the computer does not already have Agent or Virtual Appliance protection, or if the computer only has Agent protection but Virtual Appliance protection is available.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Roles

Deep Security uses role-based access control to restrict Users' access to various parts of the Deep Security system. Once you have installed the Deep Security Manager you should create individual accounts for each User and assign each User a Role that will restrict their activities to all but those necessary for the completion of their duties.

Deep Security comes pre-configured with two Roles:

- **Full Access:** The Full Access Role grants the User all possible privileges in terms of managing the Deep Security system including creating, editing, and deleting computers, computer groups, Security Profiles, Rules, Anti-Malware configurations, components, and others.
- **Auditor:** The Auditor Role gives the User the ability to view all the information in the Deep Security system but without the ability to make any modifications except to their own personal settings, such as password, contact information, dashboard layout preferences, and others.

Depending on the level of access granted, controls in the Manager interface will be either visible and changeable, visible only but disabled, or hidden. For a list of the rights granted in the pre-configured Roles, as well as the default rights settings when creating a new Role, see **Role-Based Access Control** in the **Reference** section.

You can create new Roles which can restrict Users from editing or even seeing elements of the Deep Security system such as specific computers, the properties of security Rules, or the System Settings.

Before creating User accounts, identify the Roles that your Users will take and itemize what elements of the Deep Security system those Roles will require access to and what the nature of that access will be (viewing, editing, creating, etc.). Once you have created your Roles, you can then begin creating User accounts and assigning them specific Roles.

Do not create a new Role by duplicating and then modifying the **Full Access** Role. To ensure that a new Role only grants the rights you intend, create the new Role by clicking **New** in the toolbar. The rights for a new Role are set at the most restrictive settings by default. You can then proceed to grant only the rights that are required. If you duplicate the **Full Access** Role and then apply restrictions, you risk granting some rights that you did not intend.

From the main screen you can:

- Create **New** Roles (New)
- Examine or modify the **Properties** of an existing Role ( )
- **Duplicate** (and then modify) existing Roles ( )
- **Delete** a Role ( )

Clicking **New** (New) or **Properties** ( ) displays the **Role properties window** with five tabs (**Role Properties, Computer Rights, User Rights, Configuration Rights,** and **Assigned To**).

Role Properties

General Information

The name and description of this Role.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Access Type

Select whether Users with this Role will have access to the Deep Security Manager's Web-based user interface or the Deep Security Manager's Web service API, or both.

To enable the Web service API, go to **System > System Settings > System > Web service API**.

Computer Rights

Computer and Group Rights

Use the **Computer and Group Rights** panel to confer viewing, editing, deleting, alert-dismissal, and Event tagging rights to Users in a Role. These rights can apply to all computers and computer groups or they can be restricted to only certain computers. If you wish to restrict access, select the **Selected Computers** radio button and put a check next to the computer groups and computers that Users in this role will have access to.

Four basic options are available:

- **Allow viewing of non-selected computers and data:** If Users in this role have restricted edit/delete/dismiss-alerts rights, you can still allow them to view (but not change) information about other computers by checking this box.
- **Allow viewing of events and alerts not related to computers:** Set this option to allow Users in this Role to view non-computer-related information (for example, Users being locked out, new Firewall Rules being created, IP Lists being deleted, etc.)
- **Allow new computers to be created in selected computer groups:** Set this option to Users in this Role to create new computers in the computer groups they have access to.
- **Allow sub-groups to be added/removed in selected computer groups:** Set this option to allow Users in this Role to create and delete sub-groups within the computer groups they have access to.

Advanced Rights

- **Allow computer file imports:** Allow Users in this Role to import computers using files created using the Deep Security Manager's **Computer Export** option. (See "Export Selected Computers..." on the **Computers** screen.)
- **Allow directories to be added/removed and synchronized:** Allow Users in this Role to add/remove and synchronize computers that are being managed using an LDAP-based directory like MS Active Directory.
- **Allow VMware vCenters to be added, removed and synchronized:** Allow Users in this Role to add, remove and synchronize VMware vCenters.

Security Profile Rights

Determines the rights a User in a particular Role has to create, delete, modify, or import Security Profiles.

User Rights

User Rights

The options on the **User Rights** tab allow you to set what kind of authority Users in this Role have over other Users.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **Change own password and contact information only:** Users in this Role can their own password and contact information only.
- **Create and manage Users with equal or less access:** Users in this Role can create and manage any Users who do not have any privileges greater than theirs. If there is even a single privilege that exceeds those of the Users with this Role, the Users with this Role will not be able to create or manage them.
- **Have full control over all Roles and Users:** Gives Users in this Role the ability to create and edit and Users or Roles without restrictions.

Be careful when using this option. If you assign this option to a Role, you may give a User with otherwise restricted privileges the ability to create and then sign in as a User with full unrestricted access to all aspects of the Deep Security Manager.

Custom Rights

You can further restrict "delegated" Users' ability to create/edit/delete Users and Roles using the options in the **Custom Rights** panel. Those options have the following restrictions when the **Delegate** option is selected:

- **Create:** Can only create Users with equal or lesser rights.
- **Edit:** Can only edit a User (or set/reset password) with equal or lesser rights.
- **Delete:** Can only delete Users with equal or lesser rights.

Delegate Authority

Selecting the **Delegate Authority** option will limit the authority of Users in this role. They will only be able to effect changes to Users that have equal or lesser rights than themselves. They will not be able to create, edit, or delete Roles. This ability can be further limited by deselecting any of the create/edit/delete Users options in the **Custom Rights** panel above.

Other Rights

Roles can be restricted with respect to the elements of the Deep Security system they can manipulate. Default settings for new roles are "View Only" or "Hide" for each element, but these rights can be expanded to "Full Control", or customized by choosing "Custom" from the drop-down list.

Assigned To

The **Assigned To** tab displays a list of the Users who have been assigned this Role.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Users

The term Users refers to all Deep Security Manager account holders. Use this section to create, modify, and delete User accounts. From the **Users** screen, you can:

- Create **New** User accounts (New)
- Examine or modify the **Properties** of an existing User account ( )
- Set (or change) the **Password** for a User account ( )
- **Delete** a User account ( )
- **Search** ( ) for a particular User
- **Synchronize** ( ) with an **Directory** list of Users
- View **System Events** ( ) associated with this User
- Set or change the **Role** ( ) for this User

Clicking **New** (New) or **Properties** ( ) displays the **User properties window**.

General

General Information

- **Username:** The username associated with this User's password.
- **Name:** The name of the account holder.
- **Description:** a description of the account holder.
- **Role:** Use the drop-down list to assign a pre-defined role to this User. (Assigning roles can also be done using the right-click menu when in List View mode.)

The Deep Security Manager comes pre-configured with two Roles: Full Access and Auditor. The "Full Access" role grants the User all possible privileges in terms of managing the Deep Security system such as creating, editing and deleting computers, computer groups, Security Profiles, Rules, Components, etc. The "Auditor" role gives the User the ability to ***view*** all the information in the Deep Security system but not the ability to make any modifications except to his personal settings (password, contact information, view preferences, etc.) Roles with various levels of system access rights can be created and modified in the **Roles** screen or by selecting "New..." in the **Roles** drop-down list.

- **Language:** The language that will be used in the interface when this User logs in.
- **Locked Out:** Checking this will keep this User from being able to log in to the Manager. (If a User enters the wrong password too many times when trying to log in, he will be locked out automatically. Clear this if you have resolved this situation.) (Locking or unlocking a User can also be done from the right-click menu when in List View Mode.)

Options

Click the **Set Password** button to change or assign the password for this User. Password requirements such as minimum length, upper and lower case, etc. can be set in **System > System Settings > Security.**

Contact Information

This User's contact information. Checking the **Receive Notifications** checkbox will include this User in the list of Users who receive email notifications when alerts are triggered.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Settings

Theme

- **Theme:** changes the appearance of the Deep Security Manager for this User.

Module

- **Hide Unlicensed Modules:** determines whether unlicensed modules will be hidden rather than simply grayed out for this User. (This option can be set globally on the **System > System Settings > System** screen)

Refresh Rate

- **Status Bar:** this setting determines how often the Manager's status bar refreshes during various operations such as discovering or scanning computers.
- **Alerts List/Summary:** How often to refresh the data in the **Alerts** screen in List view or Summary view.
- **Computers List:** How often to refresh the data in the **Computers** screen (if required).
- **Computer Details window:** The frequency with which an individual computer's property page refreshes itself with the latest information (if required).

List Views

- **Remember last Tag filter on each screen:** Events screens let you filter displayed events by Tag(s). This List Views setting determines if the "Tag" filter setting is retained when you navigate away from and return to an Events screen.
- **Remember last Time filter on each screen:** Events screens let you filter displayed events by Time period and computer(s). These List Views settings determine if the "Period" and "Computer" filter settings are retained when you navigate away from and return to an Events screen.
- **Remember last computer filter on each screen:** Events screens let you filter displayed events by Time period and computer(s). These List Views settings determine if the "Period" and "Computer" filter settings are retained when you navigate away from and return to an Events screen.
- **Remember last Advanced Search on each screen:** If you have performed an "Advanced Search" on an Events screen, this setting will determine if the search results are kept if you navigate away from and return to the screen.
- **Optimal number of items to show on a single page:** Screens that display lists of items will display a certain number of items per "Page". To view the next page, you must use the pagination controls. Use this setting to change the number of list-items displayed per page.
- **Maximum number of items to show on a single page:** Many lists on the Deep Security Manager are grouped into categories. For example, DPI Rules can be grouped according to Application Type. The Deep Security Manager will try to avoid splitting these groups when paginating and can override the "Optimal" setting (above) to keep items in the same group together. Use this setting to set a firm maximum on the number of items to display per page. If the number of items in a group exceeds this number, the group will be split and the group title will display information that this has been done.
- **Maximum number of items to retrieve from database:** This setting limits the number of that can retrieved from the database for display. This prevents the possibility of the Deep Security Manager getting bogged down trying to display an excessive number of results from a database query. If a query produces more than this many results, a message will appear at the top of the display informing you that only a portion of the results are being displayed.

Note that increasing these values will affect Deep Security Manager performance.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Reports

- **Enable PDF Encryption:** Determines if Reports exported in PDF format are password protected.

Reset to Default Settings: Reset all settings on this page to their defaults.

Synchronizing with a Directory

The User list can be synchronized with an Active Directory, allowing Users to log in with the password stored in the directory. Clicking **Synchronize with Directory** in the toolbar will display the **Synchronize with Directory** wizard. Type the name of the directory server and your access credentials. You will then be prompted to select which group of Users to import and whether they will be Users or Contacts. Once they've been imported, you are given the option to create a Scheduled Task to periodically synchronize with the directory to keep your list up to date. The imported list of Users are locked out of the Deep Security Manager by default. You will have to modify their Properties to allow them to log into the Manager.

Filtering the Active Directory

The first screen of the **Synchronize with Directory** wizard has an area called **Search Options** where you can write filters to specify a subset of Users to import into the Deep Security Manager. The filter language follows the Internet Engineering Task Force "Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters RFC 4515".

The default filter, "(objectClass=group)", imports all Users.

The RFC 4515 filter syntax can be used to filter for specific Users and/or Groups in a directory. For example, the following filter would import only Users who are members of an Active Directory group called "DeepSecurityUsers": "(&(objectClass=group)(cn=DeepSecurityUsers))".

The RFC 4515 definition is available at http://datatracker.ietf.org/doc/rfc4515/.

Note that the new Users, although being in the "locked out" state, have been given the "Full Access" User role.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Contacts

Users can create "Contacts". Contacts cannot login to the Deep Security Manager but they can periodically be sent reports (using Scheduled Tasks). Contacts can be assigned a "clearance" level that maps to existing Roles. When a Contact is sent a report, the report will not contain any information not accessible to a User of the same level.

From the **Contacts** screen, you can:

- Create **New** Contacts (New)
- Examine or modify the **Properties** of an existing contact ( )
- **Delete** a contact ( )
- **Synchronize** ( ) with an **Directory** list

Clicking **New** (New) or **Properties** ( ) displays the **Contact properties window**.

General Information

The name, description, and preferred language of this contact.

Contact Information

The email address entered here is the email address to which reports will sent if this contact is included in a report distribution list. (See the **Reports** screen for more information.)

Clearance

The Role specified here determines the information this contact will be allowed to see. For instance, if a computer Report has been scheduled to be sent to this contact, only information on the computers that his role permits him access to will be included in the report.

Reports

Select whether or not reports will be encrypted for this User.

Synchronizing with a Directory

The Contact list can be synchronized with an Active Directory. Clicking **Synchronize with Directory** in the toolbar will display the **Synchronize with Directory** wizard. Type the name of the directory server and your access credentials. You will then be prompted to select which group of Users to import and whether they will be Users or Contacts. Once they've been imported, you are given the option to create a Scheduled Task to periodically synchronize with the directory to keep your list up to date.

Note that the new Users, although being in the "locked out" state, have been given the "Full Access" Role.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Licenses

Displays details about your Trend Micro Deep Security product licenses. Deep Security consists of four modules: Anti-Malware, Network (Firewall/DPI), Integrity Monitoring, and Log Inspection. Each module can be licensed fully or for a trial basis. You can see an individual module's license status by clicking **View Details**. Contact Trend Micro if you wish to upgrade your license. If Trend Micro has provided you with a new activation code, click **Enter New Activation Code...** and enter it there. Newly licensed features will be immediately available.

Alerts will be raised if any module is about to expire or has expired.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Updates

This screen displays the status of current updates. To configure the source of component updates, go to **System > System Settings > Updates**.

Update Components

Anti-Malware

- **Smart Scan Agent Pattern:** The smaller malware pattern detection file that is sent to the Deep Security Virtual Appliance. If a comparison to these patterns suggests that a file on a computer may be malicious, the file is compared to the more robust pattern file on the Smart Scan server for confirmation.
- **Virus Pattern:** A file that helps the Deep Security Virtual Appliance identify virus signatures, unique patterns of bits and bytes that signal the presence of a virus.
- **IntelliTrap Pattern:** IntelliTrap searches malware that may be hidden in files that use real-time compression paired with other malware characteristics like packers.
- **IntelliTrap Exception Pattern:** The exception pattern used by IntelliTrap and the scan engines to scan for malicious code in compressed files.
- **Spyware Active-monitoring Pattern:** Spyware detection patterns.

This pattern is only used by Virtual Appliances implementing conventional scans. Virtual Appliances using Smart Scan use the Smart Scan Agent Pattern for real-time spyware scanning. The Appliances send scan queries to a Smart Scan Server if the risk of the scan target cannot be determined during scanning.

- **Virus Scan Engine:** The engine that applies virus patterns to a file during a virus scan.

Anti-Malware components are only used by the Virtual Appliance.

- **Component:** The name of the Trend Micro Anti-Malware component.
- **Current Version:** The version of the component currently downloaded to the DSM.
- **Last Updated:** When the currently downloaded component was retrieved.
- **Updated:** The sum of the number of DSVAs that have been updated with the currently downloaded component and the number of virtual machines being protected.
- **Outdated:** The sum of the number of DSVAs that have not been updated with the currently downloaded component and the number of virtual machines being protected.
- **Percent Updated:** A representation of the percentage of DSVAs and protected computers that have been updated to the latest version of the component.

DPI (Deep Packet Inspection), Integrity Monitoring, and Log Inspection

Updates to the DPI, Integrity Monitoring, and Log Inspection modules include new rules as well as modifications of existing rules.

DPI, Integrity Monitoring, and Log Inspection components are used by Virtual Appliances and Agents.

- **Component:** The name of the Trend Micro DPI, Integrity Monitoring, and Log Inspection component. (Currently there is only the Deep Security Rule Update component.)
- **Current Version:** Currently applied version of the Deep Security Rule Update.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **Last Updated:** when the Deep Security Rule Update was applied.
- **Updated:** Number of Agents/Appliances to which the Deep Security Rule Update was applied.
- **Outdated:** Number of Agents/Appliances to which the Deep Security Rule Update was not applied.
- **Percent Updated:** A representation of the percentage of Agents/Appliances/computers on which an **Update** operation has been performed subsequent to the most recent Deep Security rule update.

You can create a schedule to periodically update components automatically by toggling the **Schedule Update of Components** setting. Switching it on will start the **Scheduled Tasks** wizard.

Click the **Update Now...** button to perform an update right away. A new window is displayed listing available updates for the various Deep Security modules. Select which modules to update and click **Next** to proceed.

Click the **Apply Latest Rule Update...** button to apply the latest rule update to computers being protected by Deep Security.

The **View All Rule Updates...** button displays a list of the most recent DPI, Integrity Monitoring, and Log Inspection Rules. If required you can reapply the current Rule set to computers being protected by Deep Security or rollback to a previous Rule set. You can configure the number of Rule updates that are kept in the Deep Security Manager's database by going to the **Prune** area in the **System > System Settings > System** tab.

The **Rollback Anti-Malware...** button displays the **Anti-Malware Rollback** wizard. Use it to restore any or all the components on computers being protected by Deep Security to their previous version.

Only computers/Agents/Appliances which have undergone an update can be rolled back.

Software Packages

Available software packages will include new versions of the Manager, the Agents, the Virtual Appliance, and the Deep Security Filter Driver.

- **Package Name:** The file name of the software package (which will include the version number).
- **Latest Version:** The latest version of the software available from Trend Micro.
- **Latest Local Version:** The latest version of the software downloaded to the Manager. (The Manager can store older versions of software packages. You can configure the number of previous software versions to store in the **Prune** area on the **System > System Settings > System** screen.)
- **Updated:** Number of software components that that have been updated to the latest version *available from Trend Micro*.
- **Outdated:** Number of software components that that have not been updated to the latest version *available from Trend Micro*.
- **Percentage Updated:** A representation of the percentage of software components which have been updated to the latest version *available from Trend Micro*.

Updates to security Components, Deep Security Agents, and Deep Security Virtual Appliances can all be deployed using the Deep Security Manager. New versions of the Deep Security Manager, however, must be installed independently of your current Deep Security Manager. That is, you must download the new version from the Trend Micro Download Center, run the installer, and follow the instructions to perform a software upgrade.

You can create a schedule to periodically check for new software by toggling the **Schedule Check of Newer Software** setting. Switching it on will start the **Scheduled Tasks** wizard.

Click **Open Download Center...** to open a new browser window which will take you to the Trend Micro Download Center where Deep Security software packages are available for download.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Once you have downloaded the software packages you need, you will have to import them into the Deep Security Manager. Click **Import Software...** to import the software into the Deep Security Manager.

Click **View Imported Software...** to open a window displayed a list of downloaded and imported software.

The **Check for Newer Software** button performs an automatic check if newer versions of *currently deployed* software packages are available.

Before deploying new software, be sure to check the Trend Micro Download Center for any accompanying documentation, including Installation Guides.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

The Deep Security Virtual Appliance Interface

The Deep Security Virtual Appliance

The Deep Security Virtual Appliance interface can be accessed by opening the VMware vSphere Client, selecting the DSVA in the navigation pane, and clicking on the **Console** tab.

System Information

Displays the DSVA version number, build number, and the URL of the Deep Security Manager managing this Appliance.

Configure Password

The current password for Accessing this Appliance console. The default password ("dsva") should be changed after installation.

Configure Management Network

Displays the Appliance hostname and IP address. Initially the Appliance is given the default hostname "dsva". The IP address is assigned by the local DHCP server. If you do not have a DHCP server, you must enter the IP Address, Netmask, Default gateway, Primary DNS, and Secondary DNS information manually. (Hit Enter to enter editing mode.)

If you are deploying multiple Virtual Appliances, make sure to change the hostnames to avoid DNS problems.

Configure Time Zone

The Virtual Appliance's time zone can be changed if required.

Virtual Agents

Lists all activated Agents on the Appliance. (Deactivated Agents don't appear.)

When an Agent is first listed, it is listed under its Uniformly Unique Identification (UUID). Once selected, the listed name changes to its VMware virtual machine Name.

Reset Appliance

Deactivates the Virtual Appliance. This means that all rules are erased from the Appliance, the Appliance is unlinked from its Deep Security Manager, and it can be activated by a new Manager.

Reboot System

Reboots the Virtual Appliance. Previous configuration information is maintained.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

How To...

Add Computers to the Manager

The different ways of adding computers to the Deep Security Manager's list of managed computers.

Configure Alerts

Configuring how the Manager behaves when particular alerts are triggered.

Configure Logging

Some tips on reducing the space and resources taken up by logging.

Configure Manager to Agent/Appliance Communications

A description of Manager to Agent/Appliance communications in the Deep Security System and how to configure it.

Configure Notifications

Configuring the Manager to work with third-party notification systems.

Configure Port Scan Settings

How to set which (if any) ports are scanned during the Deep Security Manager's periodic port scans of its managed computers.

Configure Syslog Integration

How to send Deep Security's logs to a Syslog Server.

Customize the Dashboard

How to customize and save the layout of the Dashboard.

Export or Back Up Data

How to export or backup your data.

Filter SSL Data Streams

How to configure Deep Security to analyze SSL encrypted traffic.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Manually Deactivate/Stop/Start the Agent/Appliance

How to Deactivate/Stop/Start the Agent/Appliance.

Manually Upgrade the Agent on a Computer

How to Manually Upgrade the Agent on a Computer.

Secure Deep Security Manager

Some suggestions on securing the computer on which Deep Security Manager is running.

Set Up Email Alerts

Configuring email alerts.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Add Computers to the Manager

New computers can be added to your Computers List by:

- Entering the IP address or hostname directly
- Initiating a Discovery operation
- Importing a Microsoft Active Directory structure
- Importing computers from a VMware vCenter
- Importing a computer list from a previously exported file

Entering the IP Address or Hostname Directly

To enter the computer information directly, go to the **Computers** screen and click **New** in the toolbar to display the **New Computer** wizard. Type the new computer's IP address or hostname and (optionally) choose a Security Profile to assign to it from the drop-down list. Press **Next** to begin the search for the computer.

If the computer is detected and an Agent is installed and running on that computer, the computer will be added to your computer List and the Agent will be activated.

"Activating" an Agent means that the Manager communicates with the Agent sending it a unique "fingerprint". The Agent will then use this fingerprint to uniquely identify the Deep Security Manager and will not accept instructions from any other Managers that might try to contact it.

If a Security Profile has been assigned to the computer, the Profile will be deployed to the Agent and the computer will be protected with all the rules and configurations that make up the Security Profile.

If the computer is detected but no Deep Security Agent is present, you will be told that the computer can still be added to your computer list but that you still have to install an Agent on the computer. Once you install an Agent on the computer, you will have to find the computer in your computer List, right-click it, and choose "Activate/Reactivate" from the context menu.

If the computer is not detected (not visible to the Manager), you will be told that you can still add the computer but that when it becomes visible to the Manager you will have to activate it as above.

Initiating a Discovery Operation

A discovery operation scans the network for visible computers. To initiate a discovery operation, click **Discover**... in the toolbar in the **Computers** screen. The **Discover Computers** dialog will appear.

You are provided several options to restrict the scope of the scan. You can choose to perform a port scan of each discovered computer. Use this option carefully as it can take a lot of time if you are discovering/scanning a large number of computers.

When discovering computers you can specify a computer group to which they should be added. Depending on how you have chosen to organize your computer groups, it may be convenient to create a computer group called "Newly Discovered Computers", or "Newly Discovered Computers on Network Segment X" if you will be scanning multiple network segments. You can then move your discovered computers to other computer groups based on their properties and activate them.

During discovery, the Manager searches the network for any visible computers. When a computer is found, the Manager attempts to detect whether an Agent is present. When discovery is complete, the Manager displays all the computers it has detected and displays their status in the **Status** column. After discovery operations, a computer can be in one of the following states:

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **Discovered (No Agent):** The computer has been detected but no Agent is present. The computer may also be in this state if an Agent is installed but has been previously activated and is configured for Agent initiated communications. In this case, you will have to deactivate and then reactivate the Agent. ("No Agent" will also be reported if the Agent is installed but not running.)
- **Discovered (Activation Required):** The Agent is installed and listening, and has been activated, but is not yet being managed by the Manager. This state indicates that this Manager was at one point managing the Agent, but the Agent's public certificate is no longer in the Manager's database. This may be the case if the if the computer was removed from the Manager and then discovered again. To begin managing the Agent on this computer, right-click the computer and select "Activate/Reactivate". Once reactivated, the **Status** will change to "Online".
- **Discovered (Deactivation Required):** The Agent is installed and listening, but it has already been activated by another Manager. In this case the Agent must be deactivated (reset) prior to activation by this Manager. Deactivating an Agent must be done using the Manager that originally activated it or it can be reset directly on the computer. To deactivate the Agent from the Manager, right-click the computer and choose **Actions > Deactivate**.

The Discovery operation will not discover computers running as virtual machines in a vCenter or computers in a Directory/Active directory.

Importing a Microsoft Active Directory Structure

Deep Security Manager supports the discovery of computers using Active Directory. Computers are imported and synchronized according to the structure in the directory.

To import a MS Active Directory:

1. Right-click **Computers** in the Navigation pane and select "Add Directory...".
2. Type a name and description for your imported directory (it doesn't have to match that of the Active Directory), the IP and port of the Active Directory server, and finally your access method and credentials.

Note that you must include your domain name with your username in the **User Name** field.

   Click **Next** to continue.

3. The second screen of the **New Directory** wizard asks for schema details. (The default values can be left.)

The **Details** window of each computer in the Deep Security Manager has a "Description" field. To use an attribute from your Active Directory to populate that field, type its name in the **Computer Description Attribute** text box.

   Set the **Create a Scheduled Task to Synchronize this Directory** checkbox if you want to automatically keep this structure in the Deep Security Manager synchronized with your Active Directory Server. If this checkbox is selected, the **Scheduled Task** wizard will appear when you are finished adding the directory. (You can set this up later using the **Scheduled Tasks** wizard: **System > Tasks**.) Click **Next** to continue.

4. When the Manager is finished importing your directory, you will be shown a list of computers that were added. Click **Finish**.

The directory structure now appears under **Computers** in the Navigation pane.

Additional Active Directory Options

Right-clicking an Active Directory structure gives you the following options that are not available for ordinary computer groups listed under **Computers**.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- Remove Directory
- Synchronize Now

Remove Directory

When you remove a directory from the Deep Security Manager, you have the following options:

- **Remove directory and all subordinate computers/groups from DSM:** removes all traces of the directory.
- **Remove directory, but retain computer data and computer group hierarchy:** turns the imported directory structure into identically organized regular computer groups, no longer linked with the Active Directory server.
- **Remove directory, retain computer data, but flatten hierarchy:** removes links to the Active Directory server, discards directory structure, and places all the computers into the same computer group.

Synchronize Now

Synchronizes the directory structure in the Deep Security Manager with the Active Directory Server. (Remember that you can automate this procedure as a **Scheduled Task**.)

Importing Computers from a VMware vCenter

For information on importing computers from a VMware vCenter, see the Installation Guide .

Importing a Computer List from a File

Most of the elements in the Deep Security Manager can be exported and imported. Data is stored in XML format. To export a list of computers (or IP List, Security Profile, Firewall Rule, etc.), select "Export..." from the toolbar. You can choose to export all or only selected elements. To (re)import elements, select "Import..." from the "New" menu items in the toolbar.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Configure Alerts

There are just over sixty conditions that trigger Alerts in the Deep Security system. Generally Alerts exists to warn of system status anomalies like computers going offline or DPI Rules being out of date, although there are some alerts for the detection of fingerprinting scans and other security-related events. (For notifications of individual DPI and Firewall Events, consider setting up a Syslog server.)

Alerts can be viewed by going to the **Alert** screen and clicking "Configure Alerts..." at the top-right of the screen, or going to **System > System Settings > System** and clicking "View Alert Configuration".

The actions precipitated by each alert can be configured by opening the **Properties** window for the alert. Alerts can be turned on or off; their severity can be switched between Warning and Critical.

Note that Alerts cannot be configured differently for individual Security Profiles or computers. All configuration changes to an Alert's properties are global.

You may also want to configure which Users receive email alerts. Go to **System > Users**, double click an individual User, click the **Contact Information** tab, and select or de-select the "Receive Email Alerts" option.

There is also an option to specify a default email address to which all email alerts will be sent in addition to the Users configured to receive them. This option is found in the **System > System Settings > Notifications** screen.

Note that for the emails to be sent, you must configure the SMTP settings in the **System > System Settings > System** screen.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Configure Logging

By default, Deep Security Manager collects logs from the Agents/Appliances via the heartbeat. The number of computers this feature can support depends on the frequency of the heartbeat interval (every 10 minutes by default), how active your computers are, and the log settings.

Here are some tips to help maximize the effectiveness of log collection:

- Disable log collection for computers that are not of interest. Do this by going to **System > System Settings** and then the **Firewall and DPI** tab and **Log Inspection** tab in either the computers' **Details** windows or the Security Profiles' **Details** windows.
- Consider reducing the logging of Firewall Rule activity by disabling some logging options in the Stateful Configuration **Properties** window. For example, disabling the UDP logging will eliminate the "Unsolicited UDP" log entries.
- For DPI Rules the best practice is to log only dropped packets. Logging packet modifications may result in a lot of log entries.
- For DPI Rules, only include packet data (an option in the DPI Rule's **Properties** window) when you are interested in examining the source of attacks. Otherwise leaving packet data inclusion on will result in much larger log sizes.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Configure Manager to Agent/Appliance Communications

Who Initiates Communication

At the default setting (**Bi-directional**), the Agent/Appliance will initiate the heartbeat but will still listen on the Agent port for Manager connections and the Manager is free to contact the Agent/Appliance in order to perform operations as required. **Manager Initiated** means that the Manager will initiate all communications. Communication will occur when the Manager performs scheduled updates, performs heartbeat operations (below), and when you choose the **Activate/Reactivate** or **Update Now** options from the Manager interface. If you are isolating the computer from communications initiated by remote sources, you can choose to have the Agent/Appliance itself periodically check for updates and control heartbeat operations. If this is the case, select **Agent/Appliance Initiated**.

The following information is collected by the Manager during a heartbeat: the status of the drivers (on- or off-line), the status of the Agent/Appliance (including clock time), Agent/Appliance logs since the last heartbeat, data to update counters, and a fingerprint of the Agent/Appliance security configuration (used to determine if it is up to date). You can change how often heartbeats occur (whether Agent/Appliance or Manager initiated), and how many missed heartbeats can elapse before an alert is triggered.

This setting (like many other settings) can be configured at three levels: on all computers by setting a system-wide default, only on computers to which a particular Security Profile has been assigned, and on individual computers.

On the system as a whole.

1. Go to the Manager's **System > System Settings** screen and click the **Computers** tab.
2. Select "Manager Initiated", "Agent/Appliance Initiated", or "Bi-Directional" from the drop-down list in the **Communication Direction** panel.

Only on computers to which a particular Security Profile has been assigned.

1. Open the **Security Profiles Properties** screen of the Security Profile whose communications settings you want to configure.
2. Go to **System > System Settings** and go to the **Computer** tab**.**
3. In the "Direction of Deep Security Manager to Agent/Appliance communication:" drop-down menu, select one of the three options ("Manager Initiated", "Agent/Appliance Initiated", or "Bi-directional"), or choose "Inherited". If you select "Inherited", the Security Profile will inherit the setting that was specified in the Manager's **System > System Settings** screen. Selecting one of the other options will override the global selection.
4. Click **Save** to apply the changes.

Only on a Specific Computer.

1. Open the **Details** screen of the computer whose communications settings you want to configure.
2. Go to **System > System Settings** and go to the **Computer** tab**.**
3. In the "Direction of Deep Security Manager to Agent/Appliance communication:" drop-down menu, select one of the three options ("Manager Initiated", "Agent/Appliance Initiated", or "Bi-directional"), or choose "Inherited". If you select "Inherited", the computer will inherit the setting that was specified on its Security Profile's **Details** window or in the Manager's **System > System Settings** screen. Selecting one of the other options will override the Security Profile and/or the global selection.
4. Click **Save** to apply the changes.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Note that Agents/Appliances look for the Deep Security Manager on the network by the Manager's hostname. Therefore the Manager's hostname **must** be in your local DNS for Agent/Appliance initiated or bi-directional communication to work.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Configure Notifications

In addition to alert emails via SMTP and logging to the database chosen during install (internal Derby, SQL Server, or Oracle), the Deep Security system provides several ways of integrating with third party recording and notification mechanisms.

Syslog

Both the Agents/Appliances and the Manager can be instructed to send information to a Syslog server. The Agent/Appliance will send DPI and Firewall Event information, and the Manager will send System Information. To configure the Syslog settings, go to **System > System Settings > Notifications**.

Notice that there are four panels for configuring Event Notification: one for Firewall and DPI Event Notification, Integrity Monitoring Event Notification, Log Inspection Event Notification, and System Event Notification.

For information on configuring Syslog, see Configuring Syslog Integration.

SNMP

The Manager also has the option of sending System Event Notifications from the Manager to an SNMP server. Use the same screen to enter SNMP settings. The MIB file ("DeepSecurity.mib") is located in `\Trend Micro\Deep Security Manager\util.`

Scripts

If the Syslog and SNMP options do not meet your event notification requirements, it may be possible for Trend Micro to provide a solution using custom-written scripts. Please contact Trend Micro for more information.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Configure Port Scan Settings

The Deep Security Manager can be instructed to scan a computer for open ports by right-clicking the computer and selecting **Actions > Scan for Open ports**, or by clicking the **Scan for Open Ports** button in the **Firewall** screen of the computer's **Details** window (where the results of the latest scan are displayed).

(Port scans can also be initiated by right-clicking an existing computer in the **Computers** screen and choosing "Scan for Open Ports". Another way to initiate port scans is to create a **Scheduled Task** to regularly carry out port scans on a list of computers.)

By default, the range of ports that are scanned is the range known as the "Common Ports", 1-1024, but you can define a different set of ports to scan.

Port 4118 is always scanned regardless of port range settings. It is the port on the computer to which Manager initiated communications are sent. If communication direction is set to "Agent/Appliance Initiated" for a computer (**System > System Settings > Computers**), port 4118 is closed.

To define a new port range to be scanned:

1. Go to **Components > Port Lists** and click **New** in the menu bar. The **New Port List** screen will appear.
2. Type a name and description for the new port list and then define the ports in the **Port(s)** text box using the accepted formats. (For example, to scan ports 100, 105, and 110 through 120, you would type "100" on the first line "105" on the second, and "110-120" on the third.) Click **OK**.
3. Now go to **System > System Settings > Scan** and click the "Ports to Scan" drop-down menu. Your newly defined Port List will be one of the choices.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Configure Syslog Integration

Deep Security supports Common Event Format 1.0, a format sponsored by ArcSight (www.arcsight.com). Although Deep Security supports two other syslog formats (Basic Syslog, and Common Event Format (legacy)). These formats are made available for legacy installations and should not be used for new integration projects.

Enabling Syslog forwarding in the Deep Security Manager does not affect default logging. That is, enabling syslog will not "turn off" the normal logging mechanisms.

Setting up a Syslog on Red Hat Enterprise

The following steps describe how to configure Syslog on Red Hat Enterprise to receive logs from Deep Security Agents/Appliances.

1. Log in as root
2. Execute: `vi /etc/syslog.conf`
3. Add the following two lines of text to the end of the `syslog.conf`:
   - `#Save Deep Security Manager logs to DSM.log`
   - `Local4.*  /var/log/DSM.log`
4. Save the file and exit
5. Create the `/var/log/DSM.log` file by typing `touch /var/log/DSM.log`
6. Set the permissions on the DSM log so that syslog can write to it
7. Execute: `vi /etc/sysconfig/syslog`
8. Modify the line "`SYSLOGD_OPTIONS`" and add a "`-r`" to the options
9. Save the file and exit
10. Restart syslog: `/etc/init.d/syslog restart`

When Syslog is functioning you will see logs populated in: `/var/log/DSM.log`

Deep Security Manager Settings

You can configure Deep Security Manager to instruct all managed computers to send logs to the Syslog computer, or you can configure individual computers independently.

To configure the Manager to instruct all managed computers to use Syslog, go to the **System > System Settings** screen and click the **Notifications** tab. In the panel called "System Event Notification",

1. Set the "Forward System Events to a remote computer (via Syslog)" option.
2. Type the hostname or the IP address of the Syslog computer.
3. Enter which UDP port to use (usually 514).
4. Select which Syslog facility to use (Local4 from the Red Hat example above.)
5. Select the "Common Event Format 1.0" log format. (The "Basic Syslog" and "Common Event Format (legacy)" formats are listed only for legacy support and should not be used for new integrations.)

Common Event Format 1.0 is a format sponsored by ArcSight (www.arcsight.com). The specification can be requested through their Web site.

You have now configured the Deep Security Manager to instruct all existing and new computers to use remote Syslog by default.

This default setting can be overridden for specific Security Profiles and on individual computers. To override on a computer, find the computer you want to configure in the **Computers** screen and double-click it to

© Copyright 2011 Trend Micro Inc.
All rights reserved.

view its **Details** window. Got to **System > System Settings** and click the **Notifications** tab. Like many other settings on a computer, you can instruct it to inherit default settings, or override them. To instruct this computer to ignore any inheritable default settings, select the "Forward Events To :" radio button and enter the details for a different Syslog server, or to not forward logs at all. Follow the same procedure to override the setting on a Security Profile.

Parsing Syslog Messages

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

To determine whether the log entry comes from the Deep Security Manager or a Deep Security Agent, look at the "Device Product" field:

Sample Log Entry: Jan 18 11:07:53 dsmhost CEF:0|Third Brigade|**Deep Security Manager**|5.0.1659|600|Administrator Signed In|4|suser=Master...

Events that occur on a VM being protected by a Virtual Appliance but without an in-guest Agent will still be identified as coming from an "Agent".

To further determine what kind of rule triggered the event, look at the "Signature ID" and "Name" fields:

Sample Log Entry: Mar 19 15:19:15 chrisds7 CEF:0|Trend Micro|Deep Security Agent|7.0.0.2036|**123**|**Out Of Allowed Policy**|5|cn1=1...

The following "Signature ID" values indicate what kind of event has been triggered:

Signature IDs	Description
10	Custom DPI Rule
20	Log Only Firewall Rule
21	Deny Firewall Rule
30	Custom Integrity Monitoring Rule
40	Custom Log Inspection Rule
100-299	Out of "Allowed" Policy Firewall Rule
300-399	SSL Events
500-899	Stateful Configuration Events
1,000,000-1,999,999	Trend Micro DPI Rule
2,000,000-2,999,999	Trend Micro Integrity Rule
3,000,000-3,999,999	Trend Micro Log Inspection Rule

Note that all the CEF extensions described in the tables below will not necessarily be included in each log entry. As well, they may not be in the order described below. If you are using regular expressions (regex) to parse the entries, make sure your expressions do not depend on each key/value pair to be there or for the key/value pairs to be in a particular order.

Note that syslog messages are limited to 1024 characters by the syslog protocol specification. In rare cases data may be truncated if long rule and interface names are used.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Firewall Event Log Format

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Sample Log Entry (1): 03-19-2010 16:19:18 Local0.Info 10.52.116.23 Mar 19 15:19:15 chrisds7 CEF:0|Trend Micro|Deep Security Agent|7.0.0.2036|123|Out Of Allowed Policy|5|cn1=1 cn1Label=Host ID act=Deny dmac=00:0C:29:8D:F1:C9 smac=00:1C:23:01:85:37 TrendMicroDsFrameType=IP src=10.52.116.140 dst=10.52.116.23 in=62 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=24431 dpt=23 cs2=0x00 SYN cs2Label=TCP Flags cnt=1

Sample Log Entry (2): 03-19-2010 16:18:33 Local0.Info 10.52.116.23 Mar 19 15:18:31 chrisds7 CEF:0|Trend Micro|Deep Security Agent|7.0.0.2036|123|Out Of Allowed Policy|5|cn1=1 cn1Label=Host ID act=Deny dmac=00:0C:29:8D:F1:C9 smac=00:1C:23:01:85:37 TrendMicroDsFrameType=IP src=10.52.116.140 dst=10.52.116.23 in=66 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=24430 dpt=23 cs2=0x00 SYN cs2Label=TCP Flags cnt=1 TrendMicroDsPacketData=AAwpjfHJABwjAYU3CABFAAA0ZjFAAIAGl4cKNHSMCjR0F19uABefXY81AAAAAIACIADD8gAAAgQFtAEDAwIBAQQC

Extension Field	Name	Description	Examples
act	Action	The action taken by the Firewall rule. Can contain: Block, Reset, Insert, Delete, Replace or Log. If the rule or the network engine is operating in detect-only mode, the action value will be proceeded by "IDS:".	act=Block act=Reset
cn1	Host Identifier	The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.	cn1=113
cn1Label	Host ID	The friendly name label for the field cn1.	cn1Label=Host ID
cnt	Repeat Count	The number of times this event was sequentially repeated.	cnt=8
cs2	TCP Flags	(For the TCP protocol only) The raw TCP flag byte followed by the URG, ACK, PSH, RST, SYN and FIN fields may be present if the TCP header was set.	cs2=0x10 ACK cs2=0x14 ACK RST
cs2Label	TCP Flags	The friendly name label for the field cs2.	cs2Label=TCP Flags
cs3	Packet Fragmentation Information	The "DF" field will be present if the IP "Don't Fragment" bit is set. The "MF" field will be present if the "IP More Fragments" bit is set.	cs3=MF cs3=DF MF
cs3Label	Fragmentation	The friendly name label	cs3Label=Fragmentation Bits

© Copyright 2011 Trend Micro Inc.
All rights reserved.

	Bits	for the field cs3.	
cs4	ICMP Type and Code	(For the ICMP protocol only) The ICMP type and code stored in their respective order delimited by a space.	cs4=11 0 cs4=8 0
cs4Label	ICMP	The friendly name label for the field cs4.	cs4Label=ICMP Type and Code
dmac	Destination MAC Address	Destination computer network interface MAC address.	dmac= 00:0C:29:2F:09:B3
dpt	Destination Port	(For TCP and UDP protocol only) Destination computer connection port.	dpt=80 dpt=135
dst	Destination IP Address	Destination computer IP Address.	dst=192.168.1.102 dst=10.30.128.2
in	Inbound Bytes Read	(For inbound connections only) Number of inbound bytes read.	in=137 in=21
out	Outbound Bytes Read	(For outbound connections only) Number of outbound bytes read.	out=216 out=13
proto	Transport protocol	Name of the connection transportation protocol used.	proto=tcp proto=udp proto=icmp
smac	Source MAC Address	Source computer network interface MAC address.	smac= 00:0E:04:2C:02:B3
spt	Source Port	(For TCP and UDP protocol only) Source computer connection port.	spt=1032 spt=443
src	Source IP Address	Source computer IP Address.	src=192.168.1.105 src=10.10.251.231
TrendMicroDsFrameType	Ethernet frame type	Connection Ethernet frame type.	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI
TrendMicroDsPacketData	Packet data	(If include packet data is set) A Base64 encoded copy of the packet data. The "equals" character is escaped. E.g. "\="	TrendMicroDsPacketData=AA...BA\=

© Copyright 2011 Trend Micro Inc.
All rights reserved.

DPI Event Log Format

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Sample Log Entry: 03-19-2010 17:11:05 Local0.Info 10.52.116.23 Mar 19 16:10:58 chrisds7 CEF:0|Trend Micro|Deep Security Agent|7.0.0.2036|1000552|Generic Cross Site Scripting(XSS) Prevention|10|cn1=1 cn1Label=Host ID dmac=00:0C:29:8D:F1:C9 smac=00:1C:23:01:85:37 TrendMicroDsFrameType=IP src=10.52.116.140 dst=10.52.116.23 in=465 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=26362 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 act=Log cn3=22 cn3Label=DPI Packet Position cs5=22 cs5Label=DPI Stream Position cs1=XSS_Attack cs1Label=DPI Note cs6=8 cs6Label=DPI Flags TrendMicroDsPacketData=R0VUIC8IM0NTQ1JJUFQlM0VhbGVydChkb2N1bWVudC5jb2...

Extension Field	Name	Description	Examples
act	Action	The action taken by the DPI rule. Can contain: Block, Reset, Insert, Delete, Replace or Log. If the rule or the network engine is operating in detect-only mode, the action value will be proceeded by "IDS:".	act=Block
cn1	Host Identifier	The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.	cn1=113
cn1Label	Host ID	The friendly name label for the field cn1.	cn1Label=Host ID
cn3	DPI Packet Position	Position within packet of data that triggered the event.	cn3=37
cn3Label	DPI Packet Position	The friendly name label for the field cn3.	cn3Label=DPI Packet Position
cnt	Repeat Count	The number of times this event was sequentially repeated.	cnt=8
cs1	DPI Filter Note	(Optional) A note field which can contain a short binary or text note associated with the payload file. If the value of the note field is all printable ASCII characters, it will be logged as text with spaces converted to underscores. If it contains binary data, it will be logged using Base-64 encoding.	cs1=Drop_data
cs1Label	DPI Note	The friendly name label for the field cs1.	cs1Label=DPI Note

© Copyright 2011 Trend Micro Inc.
All rights reserved.

cs2	TCP Flags	(For the TCP protocol only) The raw TCP flag byte followed by the URG, ACK, PSH, RST, SYN and FIN fields may be present if the TCP header was set.	cs2=0x10 ACK cs2=0x14 ACK RST
cs2Label	TCP Flags	The friendly name label for the field cs2.	cs2Label=TCP Flags
cs3	Packet Fragmentation Information	The "DF" field will be present if the IP "Don't Fragment" bit is set. The "MF" field will be present if the "IP Mote Fragments" bit is set.	cs3=MF cs3=DF MF
cs3Label	Fragmentation Bits	The friendly name label for the field cs3.	cs3Label=Fragmentation Bits
cs4	ICMP Type and Code	(For the ICMP protocol only) The ICMP type and code stored in their respective order delimited by a space.	cs4=11 0 cs4=8 0
cs4Label	ICMP	The friendly name label for the field cs4.	cs4Label=ICMP Type and Code
cs5	DPI Stream Position	Position within stream of data that triggered the event.	cs5=128 cs5=20
cs5Label	DPI Stream Position	The friendly name label for the field cs5.	cs5Label=DPI Stream Position
cs6	DPI Filter Flags	A combined value that includes the sum of the following flag values: 1 - Data truncated – Data could not be logged. 2 - Log Overflow – Log overflowed after this log. 4 - Suppressed – Logs threshold suppressed after this log. 8 - Have Data – Contains packet data 16 - Reference Data – References previously logged data.	The following example would be a summed combination of 1 (Data truncated) and 8 (Have Data): cs6=9
cs6Label	DPI Flags	The friendly name label for the field cs6.	cs6=DPI Filter Flags
dmac	Destination MAC Address	Destination computer network interface MAC address.	dmac= 00:0C:29:2F:09:B3
dpt	Destination Port	(For TCP and UDP protocol only) Destination computer	dpt=80 dpt=135

© Copyright 2011 Trend Micro Inc.
All rights reserved.

		connection port.	
dst	Destination IP Address	Destination computer IP Address.	dst=192.168.1.102 dst=10.30.128.2
in	Inbound Bytes Read	(For inbound connections only) Number of inbound bytes read.	in=137 in=21
out	Outbound Bytes Read	(For outbound connections only) Number of outbound bytes read.	out=216 out=13
proto	Transport protocol	Name of the connection transportation protocol used.	proto=tcp proto=udp proto=icmp
Smac	Source MAC Address	Source computer network interface MAC address.	smac= 00:0E:04:2C:02:B3
Spt	Source Port	(For TCP and UDP protocol only) Source computer connection port.	spt=1032 spt=443
Src	Source IP Address	Source computer IP Address.	src=192.168.1.105 src=10.10.251.231
TrendMicroDsFrameType	Ethernet frame type	Connection Ethernet frame type.	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI
TrendMicroDsPacketData	Packet data	(If include packet data is set) A Base64 encoded copy of the packet data. The "equals" character is escaped. E.g. "\="	TrendMicroDsPacketData=AA...BA\=

System Event Log Format

Base CEF Format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Sample Log Entry (1): 03-19-2010 17:32:07 Local0.Info 10.52.116.23 Mar 19 17:32:00 chrisds7 CEF:0|Trend Micro|Deep Security Manager|7.0.1591|160|Authentication Failed|4|src=10.52.116.23 suser=MasterAdmin target=MasterAdmin msg=User password incorrect for username MasterAdmin on an attempt to sign in from 127.0.0.1

Sample Log Entry (2): 03-19-2010 17:34:38 Local0.Info 10.52.116.23 Mar 19 17:34:30 chrisds7 CEF:0|Trend Micro|Deep Security Manager|7.0.1591|300|Scan for Recommendations|4|src=10.52.116.23 suser=System target=localhost msg=A Scan for Recommendations on computer (localhost) has completed. Any changes to the computer as a result of this Scan for Recommendations will have been reflected in a 'Computer Updated' system event.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Extension Field	Name	Description	Examples
src	Source IP Address	Source Deep Security Manager IP Address.	src=10.52.116.23
suser	Source User	Source Deep Security Manager user account.	suser=MasterAdmin
target	Target entity	The event target entity. The target of the event maybe the administrator account logged into Deep Security Manager, or a Computer.	target=MasterAdmin target=server01
msg	Details	Details of the System event. May contain a verbose description of the event.	msg=User password incorrect for username MasterAdmin on an attempt to sign in from 127.0.0.1 msg=A Scan for Recommendations on computer (localhost) has completed...

Log Inspection Event Format

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Log Entry Example (1): 03-19-2010 16:47:12 Local0.Info 10.52.116.23 Mar 19 15:47:08 chrisds7 CEF:0|Trend Micro|Deep Security Agent|7.0.0.2036|3002795|Microsoft Windows Events|8|cn1=1 cn1Label=Host ID cs1Label=LI Description cs1=Multiple Windows audit failure events fname=Application duser=(no user) shost=server01 msg=WinEvtLog: Application: AUDIT_FAILURE(20187): pgEvent: (no user): no domain: CHRISDS7: Remote login failure for user 'xyz'

Log Entry Example (2): 03-19-2010 16:55:18 Local0.Info 10.52.116.23 Mar 19 15:55:13 chrisds7 CEF:0|Trend Micro|Deep Security Agent|7.0.0.2036|3002795|Microsoft Windows Events|6|cn1=1 cn1Label=Host ID cs1Label=LI Description cs1=Windows audit success event fname=Security duser=NETWORK SERVICE shost=server01 msg=WinEvtLog: Security: AUDIT_SUCCESS(552): Security: NETWORK SERVICE: NT AUTHORITY: SERVER01: Logon attempt using explicit credentials: Logged on user: <009>User Name: NETWORK SERVICE <009>Domain: <009>NT AUTHORITY <009>Logon ID: <009>(0x0,0x3E4) <009>Logon GUID: - User whose credentials were used: <009>Target User Name: IUSR_WIN2003-X86-ENT <009>Target Domain: SERVER01 <009>Target Logon GUID: - Target Server Name: localhost Target Server Info: localhost Caller Process ID: 2312 Source Network Address: - Source Port: -

Extension Field	Name	Description	Examples
cn1	Host Identifier	The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.	cn1=113
cn1Label	Host ID	The friendly name label for the field cn1.	cn1Label=Host ID
cs1	Specific Sub-Rule	The Log Inspection sub-rule which triggered this event.	cs1=Multiple Windows audit failure events
cs1Label	LI Description	The friendly name label for the field cs1.	cs1Label=LI Description
duser	User Information	(If parse-able username	duser=(no user)

© Copyright 2011 Trend Micro Inc.
All rights reserved.

		exists) The name of the target user initiated the log entry.	duser=NETWORK SERVICE
fname	Target entity	The Log Inspection rule target entity. May contain a file or directory path, registry key, etc…	fname=Application fname=C:\Program Files\CMS\logs\server0.log
msg	Details	Details of the Log Inspection event. May contain a verbose description of the detected log event.	msg=WinEvtLog: Application: AUDIT_FAILURE(20187): pgEvent: (no user): no domain: SERVER01: Remote login failure for user 'xyz'
shost	Source Hostname	Source computer Hostname	shost=webserver01.corp.com
src	Source IP Address	Source computer IP Address.	src=192.168.1.105 src=10.10.251.231

Integrity Monitoring Log Format

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Log Entry Sample: 03-19-2010 16:36:22 Local0.Info 10.52.116.23 Mar 19 15:36:18 chrisds7 CEF:0|Trend Micro|Deep Security Agent|7.0.0.2036|2002773|Microsoft Windows - 'Hosts' file modified|8|cn1=1 cn1Label=Host ID act=updated filePath=C:\WINDOWS\system32\drivers\etc\hosts msg=lastModified,sha1,size

Extension Field	Name	Description	Examples
act	Action	The action detected by the integrity rule. Can contain: created, updated, detected or renamed.	act=created act=deleted
cn1	Host Identifier	The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.	cn1=113
cn1Label	Host ID	The friendly name label for the field cn1.	cn1Label=Host ID
filePath	Target	The	filePath=C:\WINDOWS\system32\drivers\etc\hosts

© Copyright 2011 Trend Micro Inc.
All rights reserved.

	Entity	integrity rule target entity. May contain a file or directory path, registry key, etc…	
msg	Attribute changes	(For "updated" action only) A list of changed attribute names.	msg=lastModified,sha1,size
oldfilePath	Old target entity	(For "renamed" action only) The previous integrity rule target entity to capture the rename action from the previous target entity to the new, which is recorded in the filePath field.	oldFilePath=C:\WINDOWS\system32\logfiles\ds_agent.log

Anti-Malware Format

Base CEF format: CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Log Entry Sample: Aug 31 11:30:53 10.203.138.172 dsva CEF:0|Trend Micro|Deep Security Agent|7.5.0.1574|4000000|Eicar_test_file|6|cn1=154 cn1Label=Host ID filePath=C:\\virus\\ei1.txt act=Clean msg=Realtime

Extension Field	Name	Description	Examples
cn1	Host Identifier	The Agent Computer internal identifier which can be used to uniquely identify the Agent Computer from a given syslog event.	cn1=113
cn1Label	Host ID	The friendly name label for the field cn1.	cn1Label=Host ID
filepath	Filepath	The location of the target file.	filePath=C:\\virus\\ei1.txt
act	Action	The action carried out by the Anti-Mlaware engine. Possible values are: Deny Access, Quarantine, Delete, Pass, and Clean.	act=Clean act=Pass
msg	Message	The type of scan. Possible values are: Realtime, Scheduled, and Manual.	msg=Realtime msg=Scheduled

© Copyright 2011 Trend Micro Inc.
All rights reserved.

fsize	Filesize	The size of the target file in bytes.	fsize=120

© Copyright 2011 Trend Micro Inc.
All rights reserved.

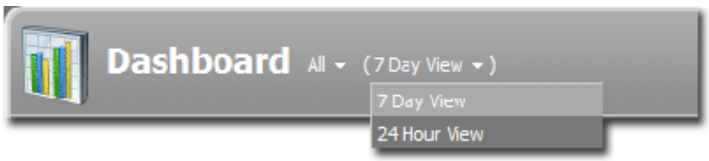
Customize the Dashboard

The Dashboard is the first screen that comes up after you log in to the Deep Security Manager. Several aspects of the dashboard can be configured and customized, and layouts can be saved and displayed when you log in. (The dashboard will be displayed as you left it when you logged out, regardless of whether another User has logged in in the meantime and made changes to their layout.)

Configurable elements of the Dashboard display are the time period the data is taken from, which computers' or computer groups' data is displayed, which "widgets" are displayed, and the layout of those widgets on the screen.

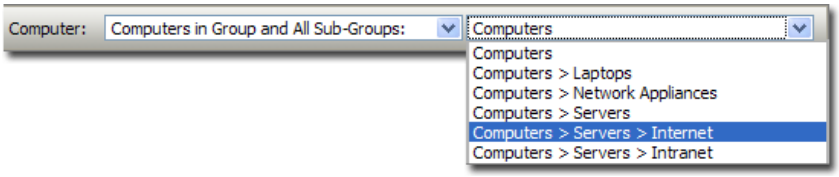
Time Period

Choose between displaying data for the last seven days or 24 hours.



Computers and Computer Groups

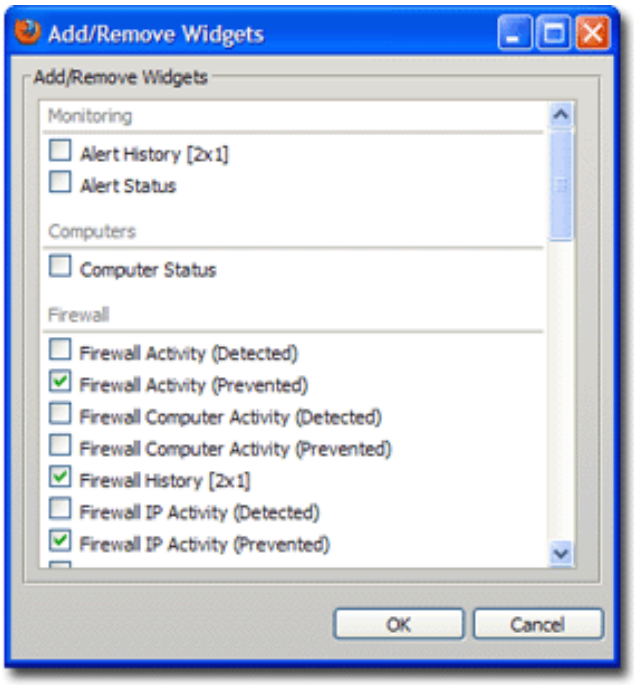
Use the **Computer:** drop-down menu to filter the displayed data to display only data from specific computers.



© Copyright 2011 Trend Micro Inc.
All rights reserved.

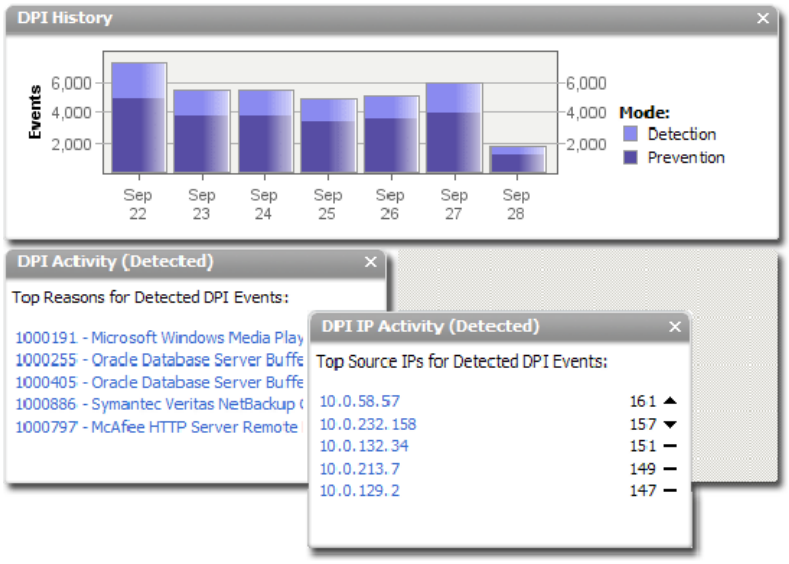
Select Dashboard Widgets

Click the **Add/Remove Widgets...** link to display the widget selection window and choose which widgets to display.



Changing the Layout

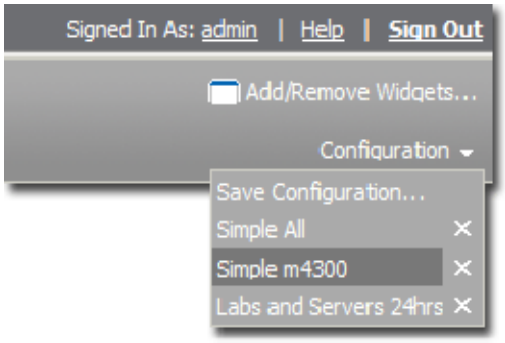
The selected widgets can be moved around the dashboard by dragging them by their title bar. Move the widget over an existing one and they will exchange places. (The widget that is about to be displaced will temporarily gray out.)



© Copyright 2011 Trend Micro Inc.
All rights reserved.

Save and Manage Dashboard Layouts

Click the **Configuration** link to save, load, or delete a dashboard layout.



© Copyright 2011 Trend Micro Inc.
All rights reserved.

Export or Back Up Data

Deep Security Manager lets you save your data in two ways: You can **backup** the Deep Security Manager's entire database, or you can **export** particular elements of the Deep Security system (logs, Firewall Rules, Stateful Configurations, computer lists, etc.).

Backup

Full database backups are for restoring your Deep Security system in the event of a catastrophic failure, or for transferring your Deep Security Manager to another computer.

Note that Deep Security Manager cannot initiate a backup of an Oracle database. To backup your Oracle database, please consult your Oracle documentation.

Internal Database or MS SQL Server Database

If you are using either the Deep Security Manager's internal database or MS SQL Server, backups can carried out using the **Scheduled Tasks** interface. Go to the **System > Tasks** screen. Click **New** and select "New Schedules Task" to display the **New Scheduled Task** wizard. Give a name to this task and choose "Backup" from the drop-down list. The next screen will prompt you for how often you want this task carried out and when. To carry out a one-time-only backup, choose "Once Only" and enter a time (5 minutes from now, for example). The next screen will prompt you for a location to store the backup files. Click through to the end of the wizard to finish. A complete backup shouldn't take more than a minute or so to complete.

A "date-named" folder will be created in the backup location you specified. If you are using the Deep Security Manager's internal database (Derby), a folder structure will be created beneath it that maps to the folders in the Deep Security Manager's install directory. To restore this database, shut down the "Trend Micro Deep Security Manager" service (using the Services Microsoft Management Console), copy the backup folders into the corresponding folders of the install directory, and restart Deep Security Manager.

If you are using a SQL Server database, two SQL Server database backup files will be written to the backup folder. For instructions on how to restore a SQL Server database, please refer to your SQL Server documentation.

Restore

Note that Deep Security Manager cannot backup or restore an Oracle database. To backup or restore your Oracle database, please consult your Oracle documentation.

Database Only

1. Stop the Deep Security Manager service
2. Restore the database (Must be a database from the same version number of the Manager)
3. Start the service
4. Verify contents restored
5. Update all of the computers to ensure they have the proper configuration

Both Deep Security Manager and Database

- Remove any remnants of the lost/corrupted Manager and database
- Install a fresh Deep Security Manager using a fresh/empty database
- Stop the Deep Security Manager service

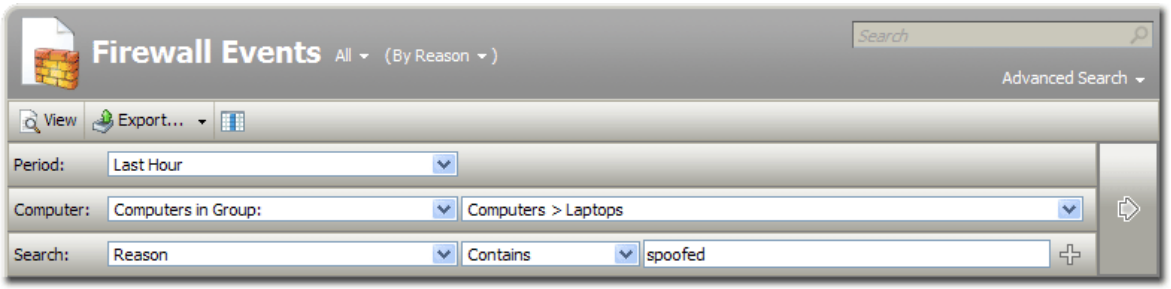
© Copyright 2011 Trend Micro Inc.
All rights reserved.

- Restore the database over the freshly installed one, must be the same database name (Must be a database from the same version number of the Manager)
- Start the Deep Security Manager service
- Verify contents restored
- Update all of the computers to ensure they have the proper configuration

Export

You can export all or various individual elements of the Deep Security System in XML or CSV format:

- **Events:** Go to one of the Events the Events screens and use the Advanced Search options to filter the Event data. For example, you could search for all **Firewall Events** for computers in the **Computers > Laptops** computer group that were logged within the **Last Hour** (the Period bar) whose **Reason** column **Contained** the word "**spoofed**" (the Search bar).



  Press the submit button (with the right-facing arrow) to execute the "query". Then press **Export** to export the filtered data in CSV format. (You can export all the displayed entries or just selected/highlighted data.) (The exporting of logs in this format is primarily for integration with third-party reporting tools.)
- **Computer Lists:** computer Lists can be exported in XML format from the **Computers** screen. You may want to do this if you find you are managing too many computers from a single Deep Security Manager and are planning to set up a second Manager to manage a collection of computers. Exporting a list of selected computers will save you the trouble of re-discovering all the computers again and arranging them into groups.

Note that Security Profile, Firewall Rule, and DPI Rule settings will *not* be included. You will have to export your Firewall Rules, DPI Rules, Stateful Configurations, and Security Profiles as well and then reapply them to your computers. See **Export All Security Components** (below) for information on exporting these elements.

- **Security Profiles:** Security profiles are exported in XML format from the **Security Profiles** screen. Once again you can filter listed items using the **Search** tool in the toolbar. The **Security Profiles** screen's **Export** button has a drop-down list next to it from which you can choose to "Export Displayed..." (meaning to export the profiles on this screen only if you have enough profiles for pagination to take effect) or "Export Selected" (meaning export only selected profiles -- you can shift-select and ctrl-select). The **Security Profiles** screen's **Export** menu gives you a third option: "Export All Security Components". See the **All Security Components** entry below for information.
- **Firewall Rules:** Firewall Rules can be exported to an XML file using the same searching/filtering techniques as above.
- **Stateful Configurations:** Stateful Configurations can be exported to an XML file using the same searching/filtering techniques as above.
- **DPI Rules:** DPI Rules can be exported to an XML file using the same searching/filtering techniques as above.
- **Integrity Monitoring Rules:** Integrity Monitoring Rules can be exported to an XML file using the same searching/filtering techniques as above.
- **Log Inspection Rules:** Log Inspection Rules can be exported to an XML file using the same searching/filtering techniques as above.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **Components:** All the reusable components (**IP Lists**, **MAC Lists**, **Port Lists**, **Application Types**, and **Schedules**) can be exported to an XML file the same way.
- **All Security Components:** You also have an option to export *all* security components at once (excluding logs and events). The drop-down list next to the **Export** button in the **Security Profiles** screen has an option to "Export All Security Components...". This option will export all of the above elements (excluding logs and events) to one XML file. (Computer Lists are not exported.)

Importing

The following instructions apply for any database being used.

To import each of the individual elements of the Deep Security System, choose "Import From File " from the drop-down list next to the **New** button in the toolbar of the elements' respective screens.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Filter SSL Data Streams

Deep Security Manager supports DPI Filtering of SSL traffic. The SSL dialog allows the User to create SSL Configurations for a given credential-port pair on one or more interfaces. Credentials can be imported in **PKCS#12** or **PEM** format, and Windows computers have the option of using **CryptoAPI** directly.

Filtering of SSL traffic is only supported by the Deep Security Agent, not the Deep Security Appliance. The Agent does not support filtering SSL connections on which SSL compression is implemented.

Configuring SSL Data Stream Filtering on a computer

Start the SSL Configuration Wizard

Open the **Details** window of the computer you wish to configure and go to **SSL Configurations** to display the **SSL Computer Configurations** screen. Click **New** to display the first page of the **SSL Configuration** wizard.

1. Select Interface(s)

Specify whether this configuration will apply to all interfaces on this computer or just one.

2. Select Port(s)

Either enter the (comma-separated) ports you want this configuration to apply to, or select a Port List.

You will also have to change the port settings on the computer's **Details** window. (See below.)

3. IP Selection

Specify whether SSL DPI analysis should take place on all IP addresses for this computer, or just one. (This feature can be used to set up multiple virtual computers on a single computer.)

4. Specify Source of Credentials

Specify whether you will provide the credentials file yourself, or whether the credentials are already on the computer.

5. Specify Type of Credentials

If you have chosen to provide the credentials now, enter their type, location, and pass phrase (if required).

If you've indicated that the credentials are on the computer, specify the type of credentials to look for.

6. Provide Credential Details

If you are using PEM or PKCS#12 credential formats stored on the computer, identify the location of the credential file and the file's pass phrase (if required).

© Copyright 2011 Trend Micro Inc.
All rights reserved.

If you are using Windows CryptoAPI credentials, choose the credentials from the list of credentials found on the computer.

7. Name and Describe this Configuration

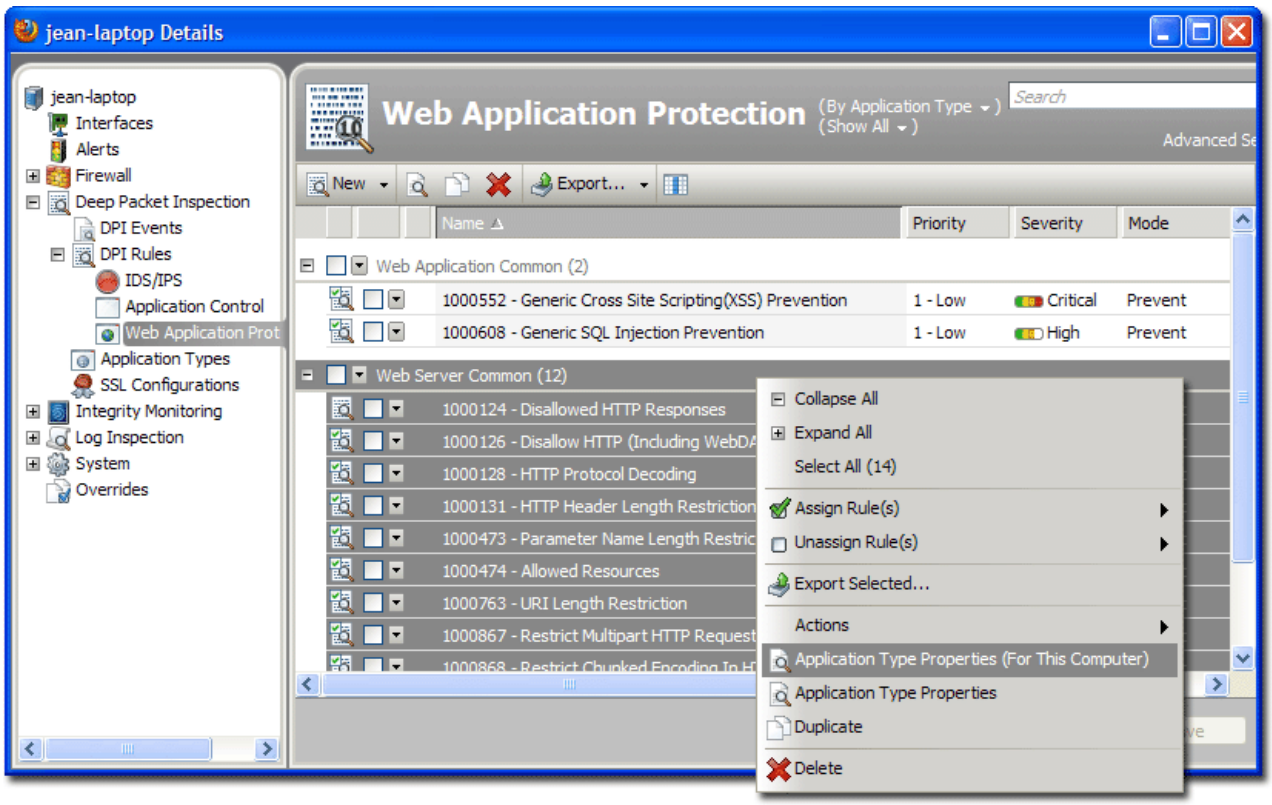
Give a name to and provide a description of this SSL configuration.

8. Look Over the Summary and Close the SSL Configuration Wizard

Read the summary of the configuration operation and click **Finish** to close the wizard.

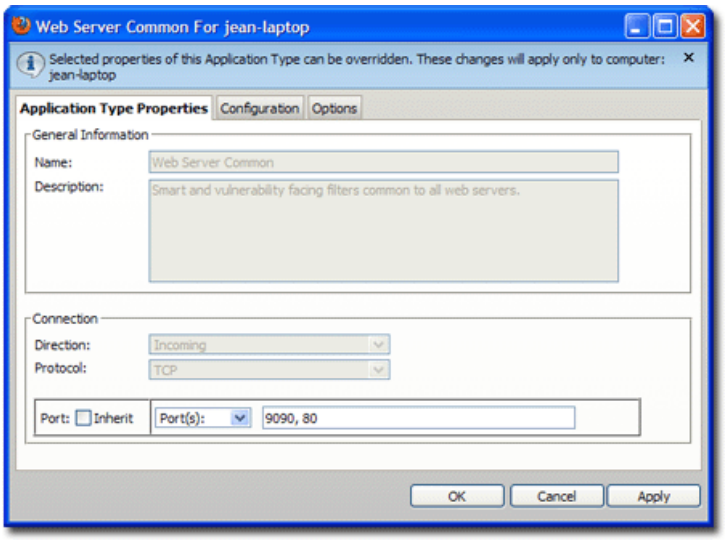
Change Port Settings in the computer Details window to Monitor SSL Ports.

Finally, you need to ensure that the Agent is performing the appropriate DPI Filtering on the SSL-enabled port(s). Go to **DPI Rules** in the computer's **Details** window to see the list of DPI Rules being applied on this computer. Sort the rules by Application Type. Scroll down the list to find the Application Type(s) running on this computer (in this example, we will use "Web Server Common").



© Copyright 2011 Trend Micro Inc.
All rights reserved.

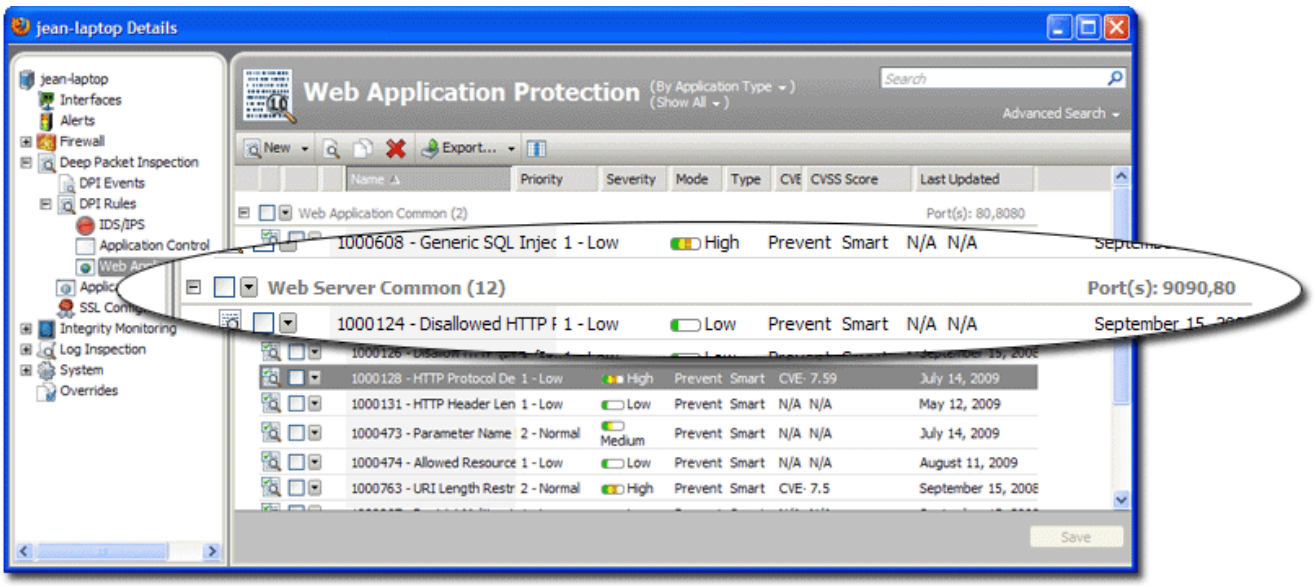
Right-click the "Web Server Common" Application Type heading and choose "Application Type Properties (For This Computer)". This will display the Application Type's **Properties** window.



Instead of using the inherited "HTTP" Port List, we will override it to include the port we defined during the SSL Configuration setup (port 9090 in this case) as well as port 80. Enter ports 9090 and 80 as comma-separated values and click **OK** to close the dialog. (Since you have selected "Application Type Properties (For This Computer)", the changes you make will only be applied to this computer. The "Web Server Common" Application Type will remain unchanged on other computers.)

The DPI Rules list in the computer's **Details** window will now refresh itself to show the changes.

Note that the Port List for The "Web Server Common" Application Type on this computer is now in **bold type**, indicating the default Port List has been overridden on this computer.



This computer is now configured for filtering SSL encrypted data streams.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Additional Notes

Note that the Deep Security Agents do not support Diffie-Hellman ciphers on Apache servers. For instructions on how to disable DH ciphers on an Apache Web server, see Disabling Diffie-Hellman in Apache.

For more detailed information on SSL support, please consult the release notes included with the Deep Security Agent software.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Manually Deactivate/Stop/Start the Agent/Appliance

Deactivating the Agent/Appliance

Deactivation of the Agent/Appliance can normally be done from the Deep Security Manager that is currently managing the Agent/Appliance. If the Deep Security Manager cannot communicate with the Agent/Appliance, you may have to perform the deactivation manually.

To deactivate the Agent on Windows:

1. From a command line, change to the Agent directory (Default is **C:\Program Files\Trend Micro\Deep Security Agent**)
2. Run the following: **dsa_control.exe /r**

To deactivate the Agent on Linux:

1. Run the following: **/etc/init.d/ds_agent reset**

To deactivate the Appliance:

- Log into vCenter using the vSphere Client.
- From the **Virtual Agents** tab, select the DSVA and view the console
- Login by pressing F2 and entering the DSVA password (default password is "dsva")
- Select **Reset Appliance**, then confirm

Stopping or Starting the Agent/Appliance

Stopping or starting the Agent/Appliance can only be done locally on the host computer.

To start or stop the Agent on Windows:

- Stop: from the command line, run the following: **sc stop ds_agent**
- Start: from the command line, run the following: **sc start ds_agent**

To start or stop the Agent/Appliance on Linux:

- Stop: run the following: **/etc/init.d/ds_agent stop**
- Start: run the following: **/etc/init.d/ds_agent start**

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Secure the Deep Security Manager

Protecting the Deep Security Manager with an Agent

Protect Deep Security Manager by installing an Agent on its host computer and apply and the **Deep Security Manager** Security Profile.

Configuring an Agent on the Deep Security Manager's computer

1. Install an Agent on the same computer as the Manager.
2. Using the **Computers** screen, add the Manager's computer (call it "localhost" or use its hostname). Do not choose to apply a Security Profile at this time.
3. Double-click the new computer in the **Computers** screen to display its **Details** window and go to **Deep Packet Inspection > SSL Configurations**.
4. A listing of the SSL Configurations for this computer will be displayed. Click **New** to start the wizard to create a new SSL Configuration.
5. Specify the interface used by the Manager. Click **Next**.
6. On the **Port** screen, choose to protect the port used by the Deep Security Manager Web Application GUI over HTTPS. (4119 by default, unless you chose another port during installation. To confirm which port the Manager is using, check the URL you're using to access it.) Click **Next**.
7. Specify whether SSL DPI analysis should take place on all IP addresses for this Computer, or just one. (This feature can be used to set up multiple virtual computers on a single computer.)
8. Next, choose to "Use the SSL Credentials built into the Deep Security Manager". (This option only appears when creating an SSL Configuration for the Manager's computer.) Click **Next**.
9. Finish the wizard and close the **SSL Configuration** screen.
10. Back in the computer's **Details** window, apply the **Deep Security Manager** Security Profile which includes the Firewall Rules and DPI Rules required for the Deep Security Manager to operate on port 4119.

You have now protected the Manager's computer and are now filtering the traffic (including SSL) to the Manager.

After configuring the Agent to filter SSL traffic, you may notice that the Deep Security Agent will return several **Renewal Error** events. These are certificate renewal errors caused by the new SSL certificate issued by the Manager computer. You should therefore restart your browser session with the Manager to acquire the new certificate from the Manager computer.

The **Deep Security Manager** Security Profile has the basic Firewall Rules assigned to enable remote use of the Manager. Additional Firewall Rules may need to be assigned if the Manager's computer is being used for other purposes. The Security Profile also includes the DPI Rules in the **Web Server Common** Application Type. Additional DPI Rules can be assigned as desired.

Because the **Web Server Common** Application Type typically filters on the **HTTP** Port List and does not include port 4119, port 4119 is added as an override to the ports setting in the **DPI Rules** screen of the Security Profile's **Details** window.

For more information on SSL data inspection, see Filter SSL Data Streams in the **How To...** section.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Set Up Email Alerts

Deep Security Manager can send emails to specific Users when selected alerts are triggered. To enable the email system, you must give Deep Security Manager access to an SMTP mail server. You must configure your SMTP settings and select which alerts will trigger emails to which Users.

Configuring your SMTP Settings

The SMTP configuration panel can be found in **System > System Settings > System**.

Type the address of your SMTP mail (with the port if required). Enter a "From" email address from which the emails should be sent. Optionally type a "bounce" address to which delivery failure notifications should be sent if the alert emails can't be delivered to one or more Users. If your SMTP mail server requires outgoing authentication, type the username and password credentials. Once you've entered the necessary information, use the **Test SMTP Settings** to test the settings.

Configuring which Alerts should Trigger Emails

There are over 30 conditions that trigger alerts and you may not want all of them to trigger the sending of an email. To configure which alerts trigger the sending of an email, go to the **System** tab in the **System > System Settings screen**. Click "View Alert Configuration" to display the list of all alerts. The checkmark next to the alert indicates whether the alert is "On" or not. If it is on, it means the alert will be triggered if the corresponding situation arises, but it does not mean an email will sent out. Double-click an alert to view its **Alert Configuration** screen.

To have an alert trigger an email, it must be turned "On" and at least one of the "Send Email" checkboxes must be selected.

Setting which Users Receive the Alert Emails

Finally, you have to set which Users receive alert emails. Go to **System > Users**. Double-click a User and select the **Contact Information** tab.

Select the "Receive Email Alerts" checkbox to have this User receive emailed notifications of alerts.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Reference

About Firewall Rules

A description of how Firewall Rules work in Deep Security.

Advanced Logging Policy Modes

To reduce the number of events being logged, the Deep Security Manager can be configured to operate in one of several Advanced Logging Policy modes.

Agent/Appliance Events

A list of all possible Agent/Appliance Events.

Bypass Rule

Information about the special "Bypass" Firewall Rule that lets certain traffic bypass the Firewall and DPI Rules.

Computer and Agent/Appliance Status

A description of various Computer and Agent/Appliance states

Creating Custom DPI Rules

Where to seek assistance in creating new DPI Rules.

Creating Custom Log Inspection Rules

Where to seek assistance in creating new Log Inspection Rules.

Creating and Applying New Firewall Rules

How to create and apply new Firewall Rules.

DPI Events

A list of explanations of the reasons displayed in the "Reason" column of DPI Event entries.

Disabling Diffie-Hellman in Apache

The Diffie-Hellman (DH) public key cryptography protocol is not supported by the Deep Security Agent and must be disabled on an Apache Web server for SSL filtering to work.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Encrypting DSM to DB Communication

How to encrypt Deep Security Manager to database communications.

Event Tagging

An explanation of the event tagging mechanism.

Firewall Events

A list of explanations of the reasons displayed in the "Reason" column of Firewall Event entries.

Firewall Rule Sequence

The order in which Firewall Rules with different priorities and actions are applied to traffic.

Inheritance and Overrides

An explanation of how settings can be inherited or overridden at various levels of the Global/Security Profile/computer hierarchy.

Integrity Monitoring Rules Language

A description of the Integrity Monitoring Rules language so you can write your own custom Integrity Monitoring Rules.

Multi Node Manager

How to set up multiple Deep Security Manager nodes to provide load balancing and redundancy.

Options for Log Inspection Rules

Configurations options for existing Log Inspection Rules.

Packet Processing Sequence

A description of the sequence in which the various elements of Deep Security are applied to the traffic stream.

Ports Used by Deep Security

Information about the ports used by Deep Security to communicate with various elements of the system.

Protecting a Mobile Laptop

A tutorial on how to protect a mobile laptop using Location Awareness.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Recommendation Scans

A description of the Recommendation Scan functionality.

Role-Based Access Control

Information on how to restrict Users' rights and privileges using Role-Based Access Control.

System Events

List of all possible System Events.

Teamed NICs

Information on installing an Agent in a teamed NIC environment.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

About Firewall Rules

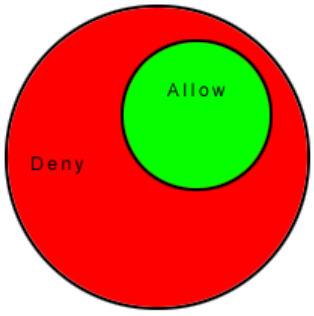
Deep Security Firewall Rules have both a rule action and a rule priority. Used in conjunction, these two properties allow you to create very flexible and powerful rule-sets. Unlike rule-sets used by other firewalls, which may require that the rules be defined in the order in which they should be run, Deep Security Firewall Rules are run in a deterministic order based on the rule action and the rule priority, which is independent of the order in which they are defined or assigned.

Rule Action

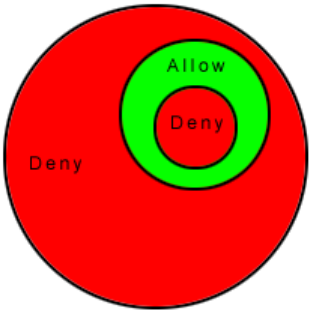
Each rule can have one of four actions.

1. **Bypass:** if a packet matches a **bypass** rule, it is passed through both the firewall *and the DPI Engine* regardless of any other rule (at the same priority level).
2. **Log Only:** if a packet matches a **log only** rule it is passed and the event is logged.
3. **Force Allow:** if a packet matches a **force allow** rule it is passed regardless of any other rules (at the same priority level).
4. **Deny:** if a packet matches a **deny** rule it is dropped.
5. **Allow:** if a packet matches an **allow** rule, it is passed. Any traffic not matching one of the **allow** rules is denied.

Adding an ALLOW rule will deny everything else:

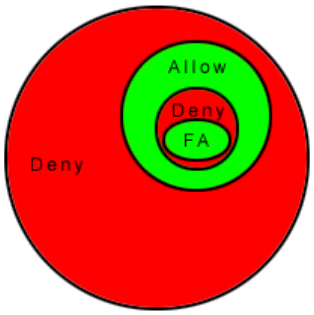


A DENY rule can be implemented over an ALLOW to block certain kinds of traffic:



© Copyright 2011 Trend Micro Inc.
All rights reserved.

The FORCE ALLOW rule can be placed over the denied traffic to allow certain exceptions to pass through:



Rule Priority

Rule actions of type **deny** and **force allow** can be defined at any one of 5 priorities to allow further refinement of the permitted traffic defined by the set of **allow** rules. Rules are run in priority order from highest (Priority 4) to lowest (Priority 0). Within a specific priority level the rules are processed in order based on the rule action (force allow, deny, allow, log only).

The priority context allows a User to successively refine traffic controls using **deny**/**force allow** combinations to achieve a greater flexibility. Within the same priority context an **allow** rule can be negated with a **deny** rule, and a **deny** rule can be negated by a **force allow** rule.

Rule Actions of type **allow** run only at priority 0 while rule actions of type **log only** run only at Priority 4.

Putting Rule Action and Priority together

Rules are run in priority order from highest (Priority 4) to lowest (Priority 0). Within a specific priority level the rules are processed in order based on the rule action. The order in which rules of equal priority are processed is as follows:

- Bypass
- Log Only
- Force Allow
- Deny
- Allow

Remember that Rule Actions of type **allow** run only at priority 0 while rule actions of type **log only** run only at priority 4.

It is important to remember that if you have a **force allow** rule and a **deny** rule at the same priority the **force allow** rule takes precedence over the **deny** rule and therefore traffic matching the **force allow** rule will be permitted.

Stateful Filtering

When stateful analysis is enabled, packets are analyzed within the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols (e.g. UDP and ICMP) a pseudo-stateful mechanism is implemented based on historical traffic analysis.

- A packet is passed through the stateful routine if it is explicitly allowed via static rules.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- The packet is examined if it belongs to an existing connection by checking the connection table for matching end points
- The TCP header is examined for correctness (e.g. sequence numbers, flag combination)

Once enabled, the stateful engine is applied to all traffic traversing the interface.

UDP pseudo-stateful inspection, by default, rejects any incoming "unsolicited" UDP packets. If a computer is running a UDP server, a **force allow** rule must be included in the policy to permit access to that service. For example, if UDP stateful inspection is enabled on a DNS server, a **force allow** rule permitting UDP traffic to port 53 is required.

ICMP pseudo-stateful inspection, by default, rejects any incoming unsolicited ICMP request-reply and error type packets. A **force allow** must be explicitly defined for any unsolicited ICMP packet to be allowed. All other ICMP (non request-reply or error type) packets are dropped unless explicitly allowed with static rules.

Putting it all together to design a Firewall Policy

Generally speaking, there are two approaches when defining a firewall policy for a computer:

- **Prohibitive:** That which is not expressly allowed is prohibited. Prohibitive policies can be created by using a combination of **allow** rules to describe allowed traffic and **deny** rules to further restrict permitted traffic.
- **Permissive:** That which is not expressly prohibited is allowed. Permissive policies can be created through the exclusive used of **deny** rules to describe the traffic that should be dropped.

In general, prohibitive policies are preferred and permissive policies should be avoided.

Force allow rules should only be used in conjunction with **allow** and **deny** rules to allow a subset of traffic that has been prohibited by the **allow** and **deny** rules. **Force allow** rules are also required to allow unsolicited ICMP and UDP traffic when ICMP and UDP stateful are enabled.

Example

Take the example of how a simple firewall policy can be created for a Web server.

1. First enable stateful inspection for TCP, UDP, and ICMP using a global stateful configuration with these options enabled.
2. Add a Firewall Rule to allow TCP and UDP replies to requests originated on the workstation. To do this create an incoming **allow** rule with the protocol set to "TCP + UDP" and select the **Not** checkbox and the **Syn** checkbox under **Specific Flags**. At this point the policy only allows TCP and UDP packets that are replies to requests initiated by a user on the workstation. For example, in conjunction with the stateful analysis options enabled in step 1, this rule allows a user on this computer to perform DNS lookups (via UDP) and to browse the Web via HTTP (TCP).
3. Add a Firewall Rule to allow ICMP replies to requests originated on the workstation. To do this, create an incoming **allow** rule with the protocol set to "ICMP" and select the **Any Flags** checkbox. This means that a user on this computer can ping other workstations and receive a reply but other users will not be able to ping this computer.
4. Add a Firewall Rule to allow incoming TCP traffic to port 80 and 443 with the **Syn** checkbox checked in the **Specific Flags** section. This means that external users can access a Web server on this computer.

At this point we have a basic firewall policy that allows solicited TCP, UDP and ICMP replies and external access to the Web server on this computer all other incoming traffic is denied.

For an example of how **deny** and **force allow** rule actions can be used to further refine this profile consider how we may want to restrict traffic from other computers in the network. For example, we may want to allow access to the Web server on this computer to internal users but deny access from any computers that are in the DMZ. This can be done by adding a **deny** rule to prohibit access from servers in the DMZ IP range.rule

© Copyright 2011 Trend Micro Inc.
All rights reserved.

5. Next we add a **deny** rule for incoming TCP traffic with source IP 10.0.0.0/24 which is the IP range assigned to computers in the DMZ. This rule denies any traffic from computers in the DMZ to this computer.

We may, however, want to refine this policy further to allow incoming traffic from the mail server which resides in the DMZ.

6. To do this we use a **force allow** for incoming TCP traffic from source IP 10.0.0.100. This **force allow** overrides the **deny** rule we created in the previous step to permit traffic from this one computer in the DMZ.

Important things to remember

- All traffic is first checked against Firewall Rules before being analyzed by the stateful inspection engine. If the traffic clears the Firewall Rules, the traffic is then analyzed by the stateful inspection engine (provided stateful inspection is enabled in the stateful configuration).
- **Allow** rules are prohibitive. Anything not specified in the **allow** rules is automatically dropped. This includes traffic of other frame types so you need to remember to include rules to allow other types of required traffic. For example, don't forget to include a rule to allow ARP traffic if static ARP tables are not in use.
- If UDP stateful inspection is enabled a **force allow** rule must be used to allow unsolicited UDP traffic. For example, if UDP stateful is enabled on a DNS server then a **force allow** for port 53 is required to allow the server to accept incoming DNS requests.
- If ICMP stateful inspection is enabled a **force allow** rule must be used to allow unsolicited ICMP traffic. For example, if you wish to allow outside ping requests a **force allow** rule for ICMP type 3 (Echo Request) is required.
- A **force allow** acts as a trump card only within the same priority context.
- If you do not have a DNS or WINS server configured (which is common in test environments) a **force allow incoming UDP port 137** rule may be required for NetBios.

When troubleshooting a new firewall policy the first thing you should do is check the Firewall Rule logs on the Agent/Appliance. The Firewall Rule logs contain all the information you need to determine what traffic is being denied by Firewall elements that have been defined so that you can further refine your policy as required.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Advanced Logging Policy Modes

To reduce the number of events being logged, the Deep Security Manager can be configured to operate in one of several **Advanced Logging Policy** modes. These modes are set in the **System > System Settings > Firewall and DPI** screen in the **Advanced** area.

The following table lists the types of Events are ignored in four of the more complex Advanced Logging Policy modes:

Mode	Ignored Events
Stateful and Normalization Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy Dropped Retransmit
Stateful, Normalization, and Frag Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy CE Flags Invalid IP Invalid IP Datagram Length Fragmented Invalid Fragment Offset First Fragment Too Small Fragment Out Of Bounds Fragment Offset Too Small IPv6 Packet Max Incoming Connections Max Outgoing Connections Max SYN Sent License Expired IP Version Unknown Invalid Packet Info Maximum ACK Retransmit Packet on Closed Connection Dropped Retransmit
Stateful, Frag, and Verifier Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy CE Flags Invalid IP Invalid IP Datagram Length Fragmented Invalid Fragment Offset First Fragment Too Small Fragment Out Of Bounds Fragment Offset Too Small IPv6 Packet Max Incoming Connections Max Outgoing Connections

© Copyright 2011 Trend Micro Inc.
All rights reserved.

	Max SYN Sent License Expired IP Version Unknown Invalid Packet Info Invalid Data Offset No IP Header Unreadable Ethernet Header Undefined Same Source and Destination IP Invalid TCP Header Length Unreadable Protocol Header Unreadable IPv4 Header Unknown IP Version Maximum ACK Retransmit Packet on Closed Connection Dropped Retransmit
Tap Mode	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Maximum ACK Retransmit Packet on Closed Connection Dropped Retransmit

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Agent/Appliance Events

Agent/Appliance Events are displayed within a System Event in the **System Events** screen. For example, double-clicking the "Events Retrieved" System Event will display a window listing all the Agent/Appliance Events that were retrieved.

Events annotated as "Deprecated" are no longer generated by the most recent Agents/Appliances but may still appear if you are running older versions.

Number	Severity	Event	Notes
0	Error	Unknown Agent/Appliance Event	
Driver-Related Events			
1000	Error	Unable To Open Engine	
1001	Error	Engine Command Failed	
1002	Warning	Engine List Objects Error	
1003	Warning	Remove Object Failed	
1004	Warning	Engine Returned Bad Rule Data	Deprecated.
Configuration-Related Events			
2000	Info	Security Configuration Updated	
2001	Warning	Invalid Firewall Rule Assignment	Deprecated.
2002	Warning	Invalid Stateful Configuration	Deprecated.
2003	Error	Save Security Configuration Failed	
2004	Warning	Invalid Interface Assignment	
2005	Warning	Invalid Interface Assignment	Deprecated.
2006	Warning	Invalid Action	
2007	Warning	Invalid Packet Direction	
2008	Warning	Invalid Rule Priority	
2009	Warning	Unrecognized IP Format	Deprecated.
2010	Warning	Invalid Source IP List	Deprecated.
2011	Warning	Invalid Source Port List	Deprecated.
2012	Warning	Invalid Destination IP List	Deprecated.
2013	Warning	Invalid Destination Port List	Deprecated.
2014	Warning	Invalid Schedule	Deprecated.
2015	Warning	Invalid Source MAC List	Deprecated.
2016	Warning	Invalid Destination MAC List	Deprecated.
2017	Warning	Invalid Schedule Length	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

2018	Warning	Invalid Schedule String	
2019	Warning	Unrecognized IP Format	Deprecated.
2020	Warning	Object Not Found	
2021	Warning	Object Not Found	
2022	Warning	Invalid Rule Assignment	
2050	Warning	Firewall Rule Not Found	Deprecated.
2075	Warning	Traffic Stream Not Found	Deprecated.
2076	Warning	DPI Rule Not Found	Deprecated.
2077	Warning	Pattern List Not Found	Deprecated.
2078	Warning	Traffic Stream Conversion Error	Deprecated.
2079	Warning	Invalid DPI Rule XML Rule	Deprecated.
2080	Warning	Conditional Firewall Rule Not Found	Deprecated.
2081	Warning	Conditional DPI Rule Not Found	Deprecated.
2082	Warning	Empty DPI Rule	Deprecated.
2083	Warning	DPI Rule XML Rule Conversion Error	Deprecated.
2085	Error	Security Configuration Error	
2086	Warning	Unsupported IP Match Type	
2087	Warning	Unsupported MAC Match Type	
2088	Warning	Invalid SSL Credential	
2089	Warning	Missing SSL Credential	
Hardware-Related Events			
3000	Warning	Invalid MAC Address	
3001	Warning	Get Event Data Failed	
3002	Warning	Too Many Interfaces	
3003	Error	Unable To Run External Command	
3004	Error	Unable To Read External Command Output	
3005	Error	Operating System Call Error	
3006	Error	Operating System Call Error	
3007	Error	File Error	
3008	Error	Machine-Specific Key Error	
3009	Error	Unexpected Agent/Appliance Shutdown	
3010	Error	Agent/Appliance Database Error	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

3300	Warning	Get Event Data Failed	Linux error.
3302	Warning	Get Security Configuration Failed	Linux error.
3303	Error	File Mapping Error	Linux error. File type error.
3600	Error	Get Windows System Directory Failed	Deprecated.
3601	Warning	Read Local Data Error	Windows error.
3602	Warning	Windows Service Error	Windows error.
3603	Error	File Mapping Error	Windows error. File size error.
3700	Warning	Abnormal Restart Detected	Windows error.
3701	Info	System Last Boot Time Change	Windows error.
Communication-Related Events			
4000	Warning	Invalid Protocol Header	Content length out of range.
4001	Warning	Invalid Protocol Header	Content length missing.
4002	Info	Command Session Initiated	
4003	Info	Configuration Session Initiated	
4004	Info	Command Received	
4011	Warning	Failure to Contact Manager	
4012	Warning	Heartbeat Failed	
Agent-Related Events			
5000	Info	Agent/Appliance Started	
5001	Error	Thread Exception	
5002	Error	Operation Timed Out	
5003	Info	Agent/Appliance Stopped	
5004	Warning	Clock Changed	
5005	Info	Agent/Appliance Auditing Started	
5006	Info	Agent/Appliance Auditing Stopped	
5007	Info	Appliance Protection Change	
5008	Warning	Filter Driver Connection Failed	
5009	Info	Filter Driver Connection Success	
5010	Warning	Filter Driver Informational Event	
Logging-Related Events			
6000	Info	Log Device Open Error	
6001	Info	Log File Open Error	
6002	Info	Log File Write Error	
6003	Info	Log Directory Creation	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

		Error	
6004	Info	Log File Query Error	
6005	Info	Log Directory Open Error	
6006	Info	Log File Delete Error	
6007	Info	Log File Rename Error	
6008	Info	Log Read Error	
6009	Warning	Log File Deleted Due To Insufficient Space	
6010	Warning	Events Were Suppressed	
6011	Warning	Events Truncated	
6012	Error	Insufficient Disk Space	
Attack/Scan/Probe-Related Events			
7000	Warning	Computer OS Fingerprint Probe	
7001	Warning	Network or Port Scan	
7002	Warning	TCP Null Scan	
7003	Warning	TCP SYNFIN Scan	
7004	Warning	TCP Xmas Scan	
Integrity Monitoring Events			
8000	Info	Full Baseline Created	Created when the Agent has been requested to build a baseline or went from 0 Integrity Monitoring Rules to n (causing the baseline to be build). This event includes information on the time taken to scan (ms), and number of entities cataloged.
8001	Info	Partial Baseline Created	Created when the Agent had a security configuration where one or more Integrity Monitoring Rules changed. This event includes information on the time taken to scan (ms), and number of entities catalogued.
8002	Info	Scan for Changes Completed	Created when the Agent is requested to do a full or partial on-demand scan. This event includes information on the time taken to scan (ms), and number of CHANGES catalogued. (Ongoing scans for changes based on the FileSystem Driver or the notify do not generate an 8002 event.)
8003	Error	Unknown Environment Variable in Integrity Monitoring Rule	Created when a rule uses a ${env.EnvironmentVar} and "EnvironmentVar" is not a known environment variable. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, and the name of the unknown environment variable.
8004	Error	Bad Base in Integrity Monitoring Rule	Created when a rule contains an invalid base directory/key. For example, specifying a FileSet with a base of "c:\foo\d:\bar" would generate this event, or the invalid value could be the result of environment variable substitution the yields a bad value. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, and the bad base value.
8005	Error	Unknown Entity in Integrity Monitoring Rule	Created when an unknown EntitySet is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, and a comma-separated list of the unknown EntitySet names encountered.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

8006	Error	Unsupported Entity in Integrity Monitoring Rule	Created when a known but unsupported EntitySet is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, and a comma-separated list of the unsupported EntitySet names encountered. Some EntitySet types such as RegistryKeySet are platform-specific.
8007	Error	Unknown Feature in Integrity Monitoring Rule	Created when an unknown Feature is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, the type of entity set (ex. FileSet), and a comma-separated list of the unknown Feature names encountered. Examples of valid Feature values are "whereBaseInOtherSet", "status", and "executable".
8008	Error	Unsupported Feature in Integrity Monitoring Rule	Created when a known but unsupported Feature is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, the type of entity set (ex. FileSet), and a comma-separated list of the unsupported Feature names encountered. Some Feature values such as "status" (used for Windows service states) are platform-specific.
8009	Error	Unknown Attribute in Integrity Monitoring Rule	Created when an unknown Attribute is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, the type of entity set (ex. FileSet), and a comma-separated list of the unknown Attribute names encountered. Examples of valid Attribute values are "created", "lastModified" and "inodeNumber".
8010	Error	Unsupported Attribute in Integrity Monitoring Rule	Created when a known but unsupported Attribute is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, the type of entity set (ex. FileSet), and a comma-separated list of the unsupported Attribute names encountered. Some Attribute values such as "inodeNumber" are platform-specific.
8011	Error	Unknown Attribute in EntitySet in Integrity Monitoring Rule	Created when an unknown EntitySet XML attribute is encountered in an Integrity Monitoring Rule. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, the type of entity set (ex. FileSet), and a comma-separated list of the unknown EntitySet attribute names encountered. You would get this event if you wrote <FileSet dir="c:\foo"> instead of <FileSet base="c:\foo">
8012	Error	Unknown Registry String in Integrity Monitoring Rule	Created when a rule references a registry key that doesn't't exist. This event includes the ID of the Integrity Monitoring Rule containing the problem, the name of the Integrity Monitoring Rule, and the name of the unknown registry string.
Log Inspection Events			
8100	Error	Log Inspection Engine Error	
8101	Warning	Log Inspection Engine Warning	
8102	Info	Log Inspection Engine Initialized	
Anti-Malware Events			

© Copyright 2011 Trend Micro Inc.
All rights reserved.

9001	Info	Anti-Malware Scan Started	
9002	Info	Anti-Malware Scan Completed	
9003	Info	Anti-Malware Scan Terminated Abnormally	
9004	Info	Anti-Malware Scan Paused	
9005	Info	Anti-Malware Scan Resumed	
9006	Info	Anti-Malware Scan Cancelled	
9007	Info	Anti-Malware Scan Cancel Failed	
9008	Info	Anti-Malware Scan Start Failed	
9009	Warning	Anti-Malware Scan Stalled	
9010	Error	Anti-Malware Quarantine Failed (VM limit exceeded)	
9011	Error	Anti-Malware Quarantine Failed (Appliance limit exceeded)	
9012	Error	Smart Scan Server Disconnected	
9013	Info	Smart Scan Server Connected	
Component Update Events			
9100	Info	Appliance Anti-Malware Component Update Success	
9101	Error	Appliance Anti-Malware Component Update Failure	Active Update runtime libraries failed to load.
9102	Error	Appliance Anti-Malware Component Update Failure	Specific information recorded in error message.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Bypass Rule

There is a special type of Firewall Rule called a Bypass Rule. It is designed for media intensive protocols where filtering may not be desired. You create a Bypass Rule by selecting "bypass" as the rule's "Action" when creating a new Firewall Rule.

The "Bypass" action on Firewall Rules differs from a Force Allow rule in the following ways:

- Packets matching Bypass will not be processed by DPI Rules
- Unlike Force Allow, Bypass will not automatically allow the responses on a TCP connection when Stateful Configuration is on (See below for more information)
- Some Bypass rules are optimized, in that traffic will flow as efficiently as if our Agent/Appliance was not there (See below for more information)

Important: When a Bypass Firewall Rule is sent to an Agent older than version 5.0, it will be treated as a Force Allow, which *will not* skip DPI Rule processing.

Using Bypass when Stateful Configuration is On

If you plan to use a Bypass Rule to skip DPI Rule processing on incoming traffic to TCP destination port N and Stateful Configuration is set to perform stateful inspection on TCP, you *must* create a matching outgoing rule for *source* port N to allow the TCP responses. (This is not required for Force Allow rules because force-allowed traffic is still processed by the stateful engine.)

All Bypass rules are unidirectional. Explicit rules are required for each direction of traffic.

Optimization

The Bypass Rule is designed to allow matching traffic through at the fastest possible rate. Maximum throughput can be achieved with (all) the following settings:

- **Priority**: Highest
- **Frame Type**: IP
- **Protocol**: TCP, UDP, or other IP protocol. (Do not use the "Any" option.)
- **Source and Destination IP and MAC**: all "Any"
- If the protocol is TCP or UDP and the traffic direction is "incoming", the Destination Ports must be one or more specified ports (not "Any"), and the Source Ports must be "Any".
- If the protocol is TCP or UDP and the traffic direction is "outgoing", the Source Ports must be one or more specified ports (Not "Any"), and the Destination Ports must be "Any".
- **Schedule**: None.

Logging

Packets that match the bypass rule will not be logged. This is not a configurable option.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Computer and Agent/Appliance Status

The **status** column of the Deep Security Manager's **Computers** screen displays the current state of the computer and its Agent/Appliance. The status column will usually display the state of the computer on the network followed by the state (in parentheses) of the Agent or Appliance providing protection if either is present. If the computer or Agent/Appliance is in an error state, that state will also be displayed in the **status** column. When operations are in progress, the status of the operation will appear in the **status** column.

The following three tables list possible status and error messages that may appear in the status column of the **Computers** screen.

In addition to the values below, the status column may also display System or Agent Events. For a list of the Events, see Agent Events and System Events in the Reference section.

Computer States

Computer State	Description	Notes
Discovered	Computer has been added to the Computers List via the Discovery process.	
Unmanaged	unactivated	
Managed	An Agent is present and activated with no pending operations or errors.	
Updating	The Agent/Appliance is being updated with a combination of new configuration settings and security updates.	
Update Pending (Schedule)	The Agent/Appliance will be updated with a combination of new configuration settings and security updates once the computer's access schedule permits.	
Update Pending (Heartbeat)	An update will be performed at the next heartbeat.	
Update Pending (Offline)	The Manager cannot currently communicate with the Agent/Appliance. An update is ready to be applied once the Agent/Appliance comes back online.	
Scanning for Open Ports	The Manager is scanning the Computer for open ports.	
Activating	The Manager is activating the Agent/Appliance.	
Activating (Delayed)	The activation of the Agent/Appliance is delayed by the amount of time specified in the relevant event-based task.	
Activated	The Agent/Appliance is activated.	
Deactivating	The Manager is deactivating the Agent/Appliance. This means that the Agent/Appliance is available for activation and management by another Deep Security Manager.	
Deactivate Pending (Heartbeat)	A deactivate instruction will be sent from the Manager during the next heartbeat.	
Locked	The computer is in a locked state. While in in a locked state the Manager will not communicate with the Agent/Appliance or generate any computer-related alerts. Existing computer alerts are not affected.	
Multiple Errors	Multiple errors have occurred on this computer. See the computer's system events for details.	
Multiple Warnings	Multiple warnings are in effect on this computer. See the computer's system events for details.	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Upgrading Agent	The Agent software on this computer is in the process of being upgraded to a newer version.	
Scanning for Recommendations	A Recommendation Scan is underway.	
Scan for Recommendations Pending (Schedule)	A Recommendation Scan will be initiated once the computer's Access Schedule permits.	
Scan for Recommendations Pending (Heartbeat)	The Manager will initiate a Recommendation Scan at the next heartbeat.	
Scan for Recommendations Pending (Offline)	The Agent/Appliance is currently offline. The Manager will initiate a Recommendation Scan when communication is reestablished.	
Integrity Scan Pending	An instruction to start an Integrity Scan is queued to be sent.	
Integrity Scan In Progress	An Integrity Scan is currently in progress.	
Integrity Scan Pending (Offline)	The Agent/Appliance is currently offline. The Manager will initiate an Integrity Scan when communication is reestablished.	
Baseline Rebuild Pending	An instruction to rebuild a system baseline for Integrity Monitoring is queued to be sent.	
Baseline Rebuild In Progress	The Integrity Monitoring engine is currently rebuilding a system baseline.	
Baseline Rebuild Pending (Offline)	The Agent/Appliance is currently offline. The Integrity Monitoring engine will rebuild a system baseline when communication between the Manager and this computer is reestablished.	
Checking Status	The agent state is being checked.	
Getting Events	The Manager is retrieving Events from the Agent/Appliance.	
Prepared	The ESX has been prepared for the installation of the Virtual Appliance. (The Filter Driver has been installed.)	ESX
Unprepared	The ESX has not been prepared for the installation of the Virtual Appliance. (The Filter Driver has been installed.)	ESX
Filter Driver Offline	The Filter Driver on the ESX is offline.	ESX
Upgrade Recommended	A newer version of the Agent or Appliance is available. An software upgrade is recommended.	ESX
Anti-Malware Manual Scan Pending	The instruction to perform an Anti-Malware Scan has not yet been sent to the Appliance.	
Anti-Malware Manual Scan Queued	The instruction to perform an Anti-Malware Scan is queued on the Appliance.	
Anti-Malware Manual Scan In Progress	A manually-initiated Anti-Malware Manual Scan is in progress.	
Anti-Malware Manual Scan Paused	A manually-initiated Anti-Malware Manual Scan has been paused.	
Anti-Malware Manual Scan Cancellation Pending	The instruction to cancel a manually-initiated Anti-Malware Scan is queued to be sent.	
Anti-Malware Manual Scan Cancellation In Progress	The instruction to cancel a manually-initiated Anti-Malware Scan has been sent.	
Anti-Malware Manual Scan Cancellation Pending (Offline)	The Appliance is offline. The instruction to cancel a manually-initiated Anti-Malware Scan will be sent when communication is reestablished.	
Anti-Malware Scheduled Scan Pending	The instruction to cancel an Anti-Malware Scan has not yet been sent to the Appliance.	
Anti-Malware Scheduled Scan Queued	The instruction to cancel an Anti-Malware Scan is queued on the Appliance.	
Anti-Malware Scheduled Scan In Progress	A scheduled Anti-Malware Manual Scan is in progress.	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Anti-Malware Scheduled Scan Paused	A scheduled Anti-Malware Manual Scan has been paused.	
Anti-Malware Scheduled Scan Cancellation Pending	The instruction to cancel a scheduled Anti-Malware Scan is queued to be sent.	
Anti-Malware Scheduled Scan Cancellation In Progress	The instruction to cancel a scheduled Anti-Malware Scan has been sent.	
Anti-Malware Scheduled Scan Cancellation Pending (Offline)	The Appliance is offline. The instruction to cancel a scheduled Anti-Malware Scan will be sent when communication is reestablished.	
Anti-Malware Manual Scan Pending (Offline)	The Appliance is offline. The instruction to start a manually-initiated Anti-Malware Scan will be sent when communication is reestablished.	
Anti-Malware Scheduled Scan Pending (Offline)	The Appliance is offline. The instruction to start a scheduled Anti-Malware Scan will be sent when communication is reestablished.	
Update of Anti-Malware Components Pending (Offline)	The Appliance is offline. The Appliance will be updated with the latest Anti-Malware Components when communication is reestablished.	
Update of Anti-Malware Components Pending (Heartbeat)	The Appliance will be updated with the latest Anti-Malware Components at the next heartbeat.	
Update of Anti-Malware Components Pending (Schedule)	Anti-Malware Components will be updated as soon as the computer's access schedule permits.	
Update of Anti-Malware Components Pending	The instruction to update Anti-Malware Components is queued to be sent.	
Update of Anti-Malware Components In Progress	The Appliance is being updated with the latest Anti-Malware Components.	

Agent States

Agent State	Description	Notes
Activated	The Agent/Appliance has been successfully activated and is ready to be managed by the Deep Security Manager.	
Activation Required	An unactivated Agent/Appliance has been detected on the target machine. It must be activated before it can be managed by the Deep Security Manager.	
VM Stopped	The virtual machine is in a "stopped" state.	
VM Paused	The virtual machine is in a "paused" state.	
No Agent/Appliance	No Agent/Appliance was detected on the ESX server.	
Unknown	No attempt has been made to determine whether an Agent/Appliance is present.	
Deactivation Required	The Manager has attempted to activate an Agent/Appliance that has already been activated by another Deep Security Manager. The original Deep Security Manager must deactivate the Agent Appliance before it can be activated by the new Manager.	
Reactivation Required	The Agent/Appliance is installed and listening and is waiting to be reactivated a Deep Security Manager.	
Online	The Agent/Appliance is online and operating as expected.	
Offline	No contact has been made with the Agent for the number of heartbeats specified in **System > Settings > Computers** screen.	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Computer Errors

Error State	Description	Notes
Communication error	General network error.	
No route to computer.	Typically the remote host cannot be reached because of an intervening firewall or if an intermediate router is down.	
Unable to resolve hostname	Unresolved socket address.	
Activation required	An instruction was sent to the Agent/Appliance when it was not yet activated.	
Unable to communicate with Agent/Appliance	Unable to communicate with Agent/Appliance .	
Protocol error	Communication failure at the HTTP layer.	
Deactivation Required	The Agent/Appliance is currently activated by another Deep Security Manager.	
No Agent/Appliance	No Agent/Appliance was detected on the target.	
No valid software version	Indicates that no installer can be found for the platform/version requested.	
Send software failed	There was an error in sending a binary package to the computer.	
Internal error	Internal error. Please contact your support provider.	
Duplicate Computer	Two computers in the Manager's Computers list share the same IP address.	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Creating Custom DPI Rules

DPI Rule Language

Deep Security provides an XML-based language designed for examining packet contents and deciding whether to log an event or reset the connection.

This document applies only to Deep Security version 5.2 and above.

Considerations for DPI Rules

DPI rules operate on network data as packets are processed in the kernel before delivery to the application (for incoming packets) or before transmission on the network (for outgoing packets). For this reason efficiency of rules is very important and DPI Rules are restricted to simple instruction like operations.

Hello World

Here is an example of a simple rule to detect the occurrence of a pattern:

```
<rule pat="hello">
    log "hello found"
</rule>
```

This `pattern-rule` is triggered by the presence of the string `hello` in a packet. When the rule is triggered the **action** block of code is executed to log an Event to the Deep Security Manager. The string "hello found" is supplied as a note in the DPI Event in the Deep Security Manager.

Note that pattern rules are case insensitive by default, i.e., this rule will trigger on any variation of the string "hello", "HELLO", "hElLo".

Note that the DPI engine does not apply pattern rules directly on raw packet data. A malicious payload could be separated into multiple segments or packet fragments, transmitted out of order or in one byte segments. The DPI engine protects against such possible attacks by analyzing the data stream before pattern rule analysis.

XML Quoting

Some characters have special meaning in XML and must be *quoted* if they are to be used in patterns or note strings. This quoting is required for the following characters:

```
< > & " '
```

Character	XML Quoting
<	<
>	>
&	&
"	"

© Copyright 2011 Trend Micro Inc.
All rights reserved.

'	'

For example to match the string one&"2" use:

```
<rule pat="one&amp;&amp;quot;2&amp;quot;">
    log "onetwo"
</rule>
```

Sometimes it may be more convenient to use hex encoded patterns. (See "More About Patterns", below.)

If these characters are not quoted properly a "Computer Updated" system error will result when they are assigned.

Application Types and Rule Directions

By default, rules are triggered as patterns found in the **forward** connection direction. The meaning of the direction depends on where the rule is to be deployed.

On a Web server listening traffic **incoming** http requests arriving on port 80 would be considered the **forward** direction and **outgoing** http responses from the Web server would be considered the **backward** direction.

On a Web client **outgoing** http requests destined for port 80 would be considered the **forward** direction whilst **incoming** replies would be the **backwards** direction.

DPI Rules can contain multiple pattern-rules that look for strings in forward or backwards direction.

```
<fwd pat="hello">log "hello found"</fwd>
<bwd pat="goodbye"> log "goodbye"</bwd>
```

Using State to Refine Rules

In the above example the "goodbye" event triggers regardless of whether "hello" has been seen or not. We can revise this rule so that "goodbye" is only significant if "hello" has already been seen:

```
<fwd pat="hello">
    stateset 1
</fwd>

<!-- this rule resets the connection when goodbye is seen after hello --
>
<bwd pat="goodbye" state="1">
    log "goodbye"
    stateset 0
</bwd>
```

These rules illustrate the use of the "stateset" action instruction and the "state" *rule constraint attribute* to implement a simple state computer that continually recognizes the occurrence of "hello" followed by "goodbye" in the reverse direction on the same connection.

Any number of pattern rules can be defined together to track state in this way.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Adding Comments

As rules start to get complex it is helpful to add comments as shown above. Comments can also be used to temporarily block out some sections when testing. Standard XML comments are used with the form `<!--  ... -->`.

More Rule Actions

Resetting a Connection (drop)

To reset a connection, use the drop instruction

```
<rule pat="bad">
    drop "bad"
</rule>
```

When a connection is reset with the "drop" instruction then no further rules will be executed on that connection or any further content even in the same packet (and the connection is reset to both endpoints and no further packets will be permitted)

Understanding Detect and Prevent Modes

A single DPI rule can be placed in detect mode. In this case a drop instruction executed by such a DPI rule is logged but does not cause the connection to be reset. Since the connection is not reset, further rules will still be executed because there may be other DPI rules that are operating in prevent mode.

Additionally, the DPI Engine can also be placed into "Detect Mode". In this mode connections are not reset but processing of further rules does stop.

Deferred Reset of a Connection (setdrop)

Sometimes it's useful to postpone the reset of a connection to allow further rules to execute.

```
<fwd pat="bad">
    setdrop "bad"
</fwd>

<fwd pat="worse">
    drop "worse"
</fwd>
```

In this case we will reset a connection if the content contains "bad" or "worse" but if it contains both then the reason will always be "worse".

As well it's possible to cancel a deferred reset:

```
<fwd pat="good">
    clrdrop
</fwd>
```

Note that `setdrop` defers the drop until the end of the packet. The occurrence of "worse" may not be the reason since that pattern may come in another packet. This is because the DPI engine does not know that "worse" is to follow and if the initial packet is determined to be malicious, it will be dropped.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

More About Rule Attributes

There are several constraint attributes that can be used to constrain a rule from triggering unless preconditions are met:

State

The `state` attribute specifies that the rule's action is only to be executed if a previous action has set the current state to the specified value. The value can be in the range 0-255.

If the state attribute is not specified then the action is triggered regardless of the current state.

Case Sensitive Matching

The `case` attribute can be used to require an exact case match:

```
<fwd pat="hello" case="1"> ... </fwd>
```

Distance Constraints

The `dist` attribute can be used to require that two patterns occur within a specified range of each other:

```
<fwd pat="hello"> ... </fwd>

<fwd pat="goodbye" dist="10,20">
    log "goodbye"
</fwd>

<fwd pat="salut" distmax="10">
    log "salut"
</fwd>

<fwd pat="ciao" distmin="10">
    log "ciao"
</fwd>
```

The first form of the attribute specifies that "goodbye" will be detected but only if it is between 10 and 20 bytes from the occurrence of another pattern.

The second form `distmax` specifies only the upper bound and no lower bound on the distance.

The last form specifies no upper bound, only a lower bound.

Note that distance constraints work with patterns in the connection direction, it is not possible to use distance constraint between a forward occurrence pattern and a backwards pattern.

Using Counters

Sometimes it is useful to trigger a rule in the absence of a pattern within a certain distance, for example, to limit the maximum size of a header field. One pattern rule can be used to start a counter, and if desired another rule can clear the counter. Counters can be used to trigger a rules without a specific pattern:

© Copyright 2011 Trend Micro Inc.
All rights reserved.

```
<fwd pat="HELLO">
    startcount 1024
</fwd>

<!-- reset if the line is longer than 256 bytes -->
<counter>
    stateset 0
</counter>

<!-- clear the counter when newline is found -->
<fwd pat="\n">
    clrcount
</fwd>
```

Only one counter can be active at a time in the same group of rules. If another counter is started while one is pending then the pending counter is automatically cleared.

Note that if a rule starts a counter, it *must* be followed by a `<counter> ...</counter>`. This is enforced by the rule compiler.

More About Patterns

Patterns are restricted to fixed length strings. These may include *wildcard* characters as follows:

\a (\A)	Alpha, a-z A-Z (non-alpha)
\w (\W)	Alphanumeric a-zA-Z0-9 (non-alpha-numeric)
\d (\D)	Digit 0-9 (non digit)
\s (\S)	Whitespace (not whitespace) [\r,\n,\t,0x32]
\p (\P)	Punctuation character, printable ascii other than above
\c (\C)	Control character, < 32, >= 127 not including whitespace
\.	Any

Special reserved or binary characters must be quoted or escaped as follows:

\xDD	Hex byte 0xDD
\\	'\' escape
|	Pipe '|' escape
|xx xx xx...|	Hex pipe (Byte sequence)

Additional rules :

- patterns cannot consist solely of wildcards
- hex encoded sequences are still case insensitive by default
- regular expression-style variable length sequences like `+`, `*` are not permitted

Examples:

```
<rule pat="|90 E8 C0 FF FF FF|/bin/sh" case="1">
    drop "IMAP overflow"
```

© Copyright 2011 Trend Micro Inc.
All rights reserved.

```
</rule>
<rule pat="port\s\d\d"> ...</rule>
```

Advanced Rule Actions

When a pattern rule triggers and the constraints are met, the rule's action is *executed*. So far we have seen the simple "log", "drop" and "stateset" actions. Actions can be used to define constraints that are more complex than those that can be expressed using the simple distance, case attributes.

Actions are defined mostly as a sequence of low level instructions. The instructions have access to a set of *virtual registers* and can perform simple arithmetic and comparison operations. Actions can also have conditional if-then-else blocks. Each instruction has one of the formats:

```
instruction STRING
instruction REG OPAND
```

For example,

```
<fwd pat="login">
    add r5 0x100 <!-- r5 <- hex 100 (=256) -->
</fwd>

<fwd pat="two">
    add r4 256 <!-- r4 <- decimal 256 -->
    load r6 r4 <!-- r6 <- -->
    <if>eq r4 r5<then/>
       log "ok"
    </if>
</fwd>
```

Register Assignments

The following virtual registers `r0-r7` and `c0-c7` are defined for use in instructions

Register #	Filter Register (r0-r7)	Connection Register (c0-c7)
0	State	Connection State
1	Cursor	UTC time/seconds
2	Reserved	Packet count
3	Reserved	Reserved
4 - 7	User defined	User defined

The state register is another way of referring to the state as used by the `state` attribute.

The `packet count register c2` register keeps track of the number of packets processed in each connection direction. The `c1` register keeps track of the current time (in seconds since 1970.) These registers can be used to express time or packet based constraints.

Additional details on registers:

- registers `c0-c3` and `r0-r3` have predefined meaning
- registers `r4-r7` can be used for any purpose

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- the connection registers `c0-c7` are shared across all rules on the same connection (each connection has it's own set)
- the registers `r0-r7` are private to each group of rules in a DPI Rule
- all registers can contain 32 bit values

Accessing Registers

Values can be put in registers and moved between registers using the `load` instruction:

```
<rule pat="test">
    load r4 100 <!-- load value 100 decimal into r4 -->
    load r5 r4 <!-- copy contents of register r4 into r5 -->
</rule>
```

Since `r0` is the state register, the `stateset` instruction is really just a shorthand for the `load instruction`; the following are equivalent:

```
<rule pat="test">
    load r0 1 stateset 1 <!-- same as above -->
</rule>
```

Comparing Registers

Registers can be compared using `if` blocks and comparison instructions. For example the following rule will reset a connection when the pattern "login" occurs more than three times:

```
<rule pat="login">
   add r4 1
   <if>
      gt r4 3<then/>
      drop "repeated3"
   </if>
</rule>
```

if-Statement

The `if` statement has the general format:

```
<if> (condition) <then/>
    <!-- if blocks can be nested -->
    <if> (condition) <then/>
       (statements)
</if>


<elseif/> (else condition) <then/>
    (elseif statements)
<else/>
    (else statements) </if>
```

break

© Copyright 2011 Trend Micro Inc.
All rights reserved.

The `break` instruction stops processing further instructions for the action. This is sometimes helpful to simplify a nested `if-block`

```
<if>lt r4 0<then/>
    break
</if>

<if>gt r4 10<then/>
    drop "range"
</if>
```

The following instructions can be used to compare registers:

Equality

Instruction	True If
eq	REG == OPERAND
!eq	REG != OPERAND

Signed Comparison

The following instructions perform comparison, treating the register and operand as signed 32 bit quantities:

gt	True if REG > OPERAND
!gt	True if REG <= OPERAND
lt	True if REG < OPERAND
!lt	True if REG >= OPERAND

Unsigned Comparison

The following instructions perform comparison, treating the register and operand as unsigned 32 bit quantities:

ugt	Unsigned: REG > OPERAND
!ugt	Unsigned: REG <= OPERAND
ult	Unsigned: REG < OPERAND
!ult	Unsigned: REG >= OPERAND

Modulo32 Comparison

The following instructions treat the register and operand as modulo32 quantities. Protocols like TCP use sequence numbers that wrap around across 32 bit boundaries.

mlt	Mod32: REG < OPERAND
!mlt	Mod32: REG >= OPERAND
mgt	Mod32: REG > OPERAND

© Copyright 2011 Trend Micro Inc.
All rights reserved.

!mgt	Mod32: REG <= OPERAND

Basic Arithmetic Instructions

The arithmetic instructions allow for addition, subtraction, multiplication, division and modulo (remainder) operations:

add	REG += OPERAND
sub	REG -= OPERAND
mul	REG *= OPERAND
div	REG /= OPERAND
mod	REG %= OPERAND

Bitwise Instructions

The bitwise logical instructions treat the operand and registers as a set of 32 bits:

and	REG &= OPERAND	bitwise and
or	REG |= OPERAND	bitwise or
xor	REG ^= OPERAND	bitwise exclusive or
shiftl	REG <<= OPERAND	bitshift left (zero filled)
shiftr	REG >>= OPERAND	bitshift right (zero filled)

Order Of Execution

The DPI Engine analyzes all patterns simultaneously and executes them according to the order of pattern occurrence in the traffic stream. The engine stops processing all rules after a connection is reset, so in the case that there are two rules that might drop a connection, only the first one of these will be executed and the possible effect of the second one is masked.

If two patterns might occur at the same *position* then the engine will execute the rules in order of definition:

```
<rule pat="goodbye">drop "goodbye"</rule>
<rule pat="bye">drop "bye"</rule>
```

In this example the first defined rule will always execute before the second rule.

If the pattern rules are defined in separate DPI Rules then the order of definition can be controlled through priorities in DSM; patterns in higher priorities rules will execute before patterns in lower priorities *at the same position*.

UDP Pseudo Connections

Rules can be assigned to UDP traffic as well as TCP traffic. UDP traffic is not connection oriented by definition however request-response sequences between the same source/destination IPs and ports can be inspected in a similar way to TCP data. The following differences apply:

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- UDP messages are never re-ordered by the DPI engine
- UDP pseudo connections cannot explicitly be reset like TCP

If a rule uses the drop instruction on a UDP pseudo connection, then traffic will be blocked between these endpoints for the UDP timeout period (default 10 seconds).

Web Rules for URIs

Standard Rules can be written to check for access to particular Web server resources. However the same URI can be encoded in many different ways, for example all the following are the same:

```
http://server/index.html
http://server/./index.html
http://server/index%2ehtml
http://server/i%6edex.html
```

The DPI engine provides support for *normalizing* URIs. This feature is only enabled when the Web Protocol Decoding rules are assigned.

The following pattern rules apply only to URIs after they have been normalized, this rule will match all the above encodings:

```
<uri pat="index">
    log "index"
</uri>
```

It is not necessary to constrain these rules from executing in the HTTP body or header using additional rules. The Web decoding rules take care of tracking the state of the HTTP protocol.

Web Resource and Query Rules

Sometimes it is useful to distinguish between the first part of a URI before a `?` and the parameter part following the query. `uri` rules only run on the part of the URI before the `?`. To match on parameters use the `uriquery` rule:

```
<uriquery pat="client=firefox">
   log "firefox"
</uriquery>
```

URI parameters can be encoded in the body of an `HTTP POST` request. `uriquery` rules match the parameters in the post body as well as the part of the URI after the `?`.

Considerations for Web Rules

Be careful about mixing `uri` rules with normal rules and using state. URI rules are executed after decoding and normalization of the URI. The URI in the request line is generally not decoded until the full request line, however other rules on the raw traffic can still be executed. If there are patterns that match on the raw request line, then these will generally be triggered before the `uri` rules.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Creating Custom Log Inspection Rules

The Deep Security Log Inspection module lets you collect and analyze operating system and application logs to identify important security events buried in 1000's of log entries. These events can be sent to a security information and event management (SIEM) system, or centralized logging server for correlation, reporting, and archiving. All events are also securely collected centrally at Deep Security Manager.

The Deep Security Log Inspection module lets you:

- Meet PCI DSS Log Monitoring requirements.
- Detect suspicious behavior.
- Collect events across heterogeneous environments containing different operating systems and diverse applications.
- View events such as error and informational events (disk full, service start/shutdown, etc.).
- Create and maintain audit trails of administrator activity (administrator login/logout, account lockout, policy change, etc.).

Deep Security Log Inspection automates the collection of important security events in a number of ways:

- **Recommendation Scan:** The Recommendation Scan not only recommends DPI rules necessary to shield system and application vulnerabilities, it can also recommend Log Inspection rules for the server being scanned (i.e. Windows Log Inspection rules vs. Unix Log Inspection rules, etc.).
- **Default Log Inspection Rules:** Deep Security ships with many pre-defined rules covering a wide variety of operating systems and applications.
- **Auto-Tagging:** Log Inspection events are "auto-tagged" based upon their grouping in the log file structure. This simplifies and automates the processing of Log Inspection events within Deep Security Manager. (This feature can be turned off on the **System > System Settings > Log Inspection** screen. Turning off auto-tagging of specific events associated with user-created rules can be done on the **System > Tags** screen. Remember that a tag will not appear on that screen until the rule it is associated with has been triggered at least once.)

The Log Inspection module monitors specified log files in real time and reacts to changes to the files as they occur. It is important to remember that *if the Agent is turned off for a period of time and then turned back on, changes to the log files will not be detected by the Log Inspection module.* (Unlike the Integrity Monitoring module which builds a baseline, and then periodically scans specified files and system components and compares them to the baseline.)

Although Deep Security ships with Log Inspection Rules for many common operating systems and applications, you also have the option to create your own custom Rules. To create a custom Rule, you can either use the "Basic Rule" template, or you can write your new Rule in XML. This article will describe the Log Inspection Rule language and provide an example of a custom written rule. For a description of the properties of existing Log Inspection Rules, see the documentation for the Log Inspection Rules as well as Options for Log Inspection Rules in the **Reference** section.

The Log Inspection Process

Decoders

A Log Inspection Rule consists of a list of files to monitor for changes and a set of conditions to be met for the Rule to trigger. When the Log Inspection engine detects a change in a monitored log file, the change is parsed by a decoder. Decoders parse the raw log entry into the following fields:

- **log:** the message section of the event
- **full_log:** the entire event
- **location:** where the log came from

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **hostname:** hostname of the vent source
- **program_name:** Program name. This is taken from the syslog header of the event
- **srcip:** the source IP address within the event
- **dstip:** the destination IP address within the event
- **srcport:** the source port within the event
- **dstport:** the destination port within the event
- **protocol:** the protocol within the event
- **action:** the action taken within the event
- **srcuser:** the originating user within the event
- **dstuser:** the destination user within the event
- **id:** any ID decoded as the ID from the event
- **status:** the decoded status within the event
- **command:** the command being called within the event
- **url:** the URL within the event
- **data:** any additional data extracted from the event
- **systemname:** the system name within the event

Rules examine this decoded data looking for information that matches the conditions defined in the Rule.

If the matches are at a sufficiently high severity level, any of the following actions can be taken:

- An Alert can be raised. (Configurable on the **Options** tab of the Log Inspection Rule's **Properties** window.)
- The Event can be written to syslog. (Configurable on the Log Inspection tab in the **System > System Settings** screen.)
- The Event can sent to the Deep Security Manager. (Configurable on the Log Inspection tab in the **System > System Settings** screen.)

Log Inspection Rules

The Log Inspection engine applies Log Inspection Rules to a computer's log entries to determine if any of those entries warrant the generation of a Log Inspection Event.

A single Log Inspection Rule can contain multiple subrules. These subrules can be of two types: atomic or composite. An atomic rule evaluates a single event and a composite rule examines multiple events and can evaluate frequency, repetition, and correlation between events.

Atomic Rules

Groups

Each rule, or grouping of rules, must be defined within a **<group></group>** element. The attribute name must contain the rules you want to be a part of this group. In the following example we have indicated that our group contains the syslog and sshd rules:

```
<group name="syslog,sshd,">
</group>
```

Notice the trailing comma in the group name. Trailing commas are required if you intend to use the **<if_group></if_group>** tag to conditionally append another sub-rule to this one.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

When a set of Log Inspection Rules are sent to an Agent, the Log Inspection engine on the Agent takes the XML data from each assigned rule and assembles it into what becomes essentially a single long Log Inspection Rule. Some group definitions are common to all Log Inspection Rules written by Trend Micro. For this reason Trend Micro has included a rule called "Default Rules Configuration" which defines these groups and which always gets assigned along with any other Trend Micro rules. (If you select a rule for assignment and haven't also selected the "Default Rules Configuration" rule, a notice will appear informing you that the rule will be assigned automatically.) *If you create your own Log Inspection Rule and assign it to a Computer without assigning any Trend Micro-written rules, you must either copy the content of the "Default Rules Configuration" rule into your new rule, or also select the "Default Rules Configuration" rule for assignment to the Computer.*

Rules, ID, and Level

A group can contain as many rules as you require. The rules are defined using the **<rule></rule>** element and must have at least two attributes, the **id** and the **level**. The **id** is a unique identifier for that signature and the **level** is the severity of the alert. In the following example, we have created two rules, each with a different rule id and level:

```
<group name="syslog,sshd,">
  <rule id="100120" level="5">
  </rule>
  <rule id="100121" level="6">
  </rule>
</group>
```

Custom rules must have ID values between 100,000 to 119,999.

You can define additional subgroups within the parent group using the **<group></group>** tag. This subgroup can reference any of the groups listed in the following table:

Group Type	Group Name	Description
Reconnaissance	connection_attempt web_scan recon	Connection attempt Web scan Generic scan
Authentication Control	authentication_success authentication_failed invalid_login login_denied authentication_failures adduser account_changed	Success Failure Invalid Login Denied Multiple Failures User account added User Account changed or removed
Attack/Misuse	automatic_attack exploit_attempt invalid_access spam multiple_spam sql_injection attack virus	Worm (nontargeted attack) Exploit pattern Invalid access Spam Multiple spam messages SQL injection Generic attack Virus detected
Access Control	access_denied access_allowed unknown_resource firewall_drop multiple_drops client_misconfig client_error	Access denied Access allowed Access to nonexistent resource Firewall drop Multiple firewall drops Client misconfiguration Client error
Network Control	new_host ip_spoof	New host detected Possible ARP spoofing

© Copyright 2011 Trend Micro Inc.
All rights reserved.

System Monitor	service_start system_error system_shutdown logs_cleared invalid_request promisc policy_changed config_changed low_diskspace time_changed	Service start System error Shutdown Logs cleared Invalid request Interface switched to promiscuous mode Policy changed Configuration changed Low disk space Time changed

If event auto-tagging is enabled, the event will be labeled with the group name. Log Inspection Rules provided by Trend Micro make use of a translation table that changes the group to a more user-friendly version. So, for example, "login_denied" would appear as "Login Denied". Custom rules will be listed by their group name as it appears in the rule.

Description

Include a **<description></description>** tag. The description text will appear in the event if the rule is triggered.

```
<group name="syslog,sshd,">
  <rule id="100120" level="5">
    <group>authentication_success</group>
    <description>SSHD testing authentication success</description>
  </rule>
  <rule id="100121" level="6">
    <description>SSHD rule testing 2</description>
  </rule>
</group>
```

Decoded As

The **<decoded_as></decoded_as>** tag instructs the Log Inspection engine to only apply the rule if the specified decoder has decoded the log.

```
<rule id="100123" level="5">
  <decoded_as>sshd</decoded_as>
  <description>Logging every decoded sshd message</description>
</rule>
```

To view the available decoders, go to **Log Inspection > Log Inspection Decoders**. Right-click on **1002791-Default Log Decoders** and select **Properties...**. Go the **Configuration** tab and click **View Decoders...**.

Match

To look for a specific string in a log, use the **<match></match>**. Here is a Linux sshd failed password log:

```
  Jan 1 12:34:56 linux_server sshd[1231]: Failed password for invalid
user jsmith from 192.168.1.123 port 1799 ssh2
```

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Use the **<match></match>** tag to search for the "password failed" string.

```
<rule id="100124" level="5">
  <decoded_as>sshd</decoded_as>
  <match>^Failed password</match>
  <description>Failed SSHD password attempt</description>
</rule>
```

Notice the regex caret ("^") indicating the beginning of a string. Although "Failed password" does not appear at the beginning of the log, the Log Inspection decoder will have broken up the log into sections. (See "Decoders", above.) One of those sections is "log" which is the message part of the log (as opposed to "full_log" which is the log in its entirety.)

The following table lists supported regex syntax:

Regex Syntax	Description
\w	A-Z, a-z, 0-9 single letters and numerals
\d	0-9 single numerals
\s	single space
\t	single tab
\p	()*+,-.:;<=>?[]
\W	not \w
\D	not \d
\S	not \s
\.	anything
+	match one or more of any of the above (for example, \w+, \d+)
*	match zero or more of any of the above (for example, \w*, \d*)
^	indicates the beginning of a string (^somestring)
$	specify the end of a string (somestring$)
|	indicate an "OR" between multiple strings

Conditional Statements

Rule evaluation can be conditional upon other rules having been evaluated as true. The **<if_sid></if_sid>** tag instructs the Log Inspection engine to only evaluate this subrule if the rule identified in the tag has evaluated as true. The following example shows three rules: 100123, 100124, and 100125. Rules 100124 and 100125 have been modified to be children of the 100123 rule using the **<if_sid></if_sid>** tag:

```
<group name="syslog,sshd,">
  <rule id="100123" level="2">
    <decoded_as>sshd</decoded_as>
    <description>Logging every decoded sshd message</description>
  </rule>
  <rule id="100124" level="7">
    <if_sid>100123</if_sid>
    <match>^Failed password</match>
    <group>authentication_failure</group>
```

© Copyright 2011 Trend Micro Inc.
All rights reserved.

```
    <description>Failed SSHD password attempt</description>
  </rule>
  <rule id="100125" level="3">
    <if_sid>100123</if_sid>
    <match>^Accepted password</match>
    <group>authentication_success</group>
    <description>Successful SSHD password attempt</description>
  </rule>
</group>
```

Hierarchy of Evaluation

The **<if_sid></if_sid>** tag essentially creates a hierarchical set of rules. That is, by including an **<if_sid></if_sid>** tag in a rule, the rule becomes a child of the rule referenced by the **<if_sid></if_sid>** tag. Before applying any rules to a log, the Log Inspection engine assesses the **<if_sid></if_sid>** tags and builds a hierarchy of parent/child rules.

The hierarchical parent/child structure can be used to improve the efficiency of your rules. If a parent rule does not evaluate as true, the Log Inspection engine will ignore the children of that parent.

Although the **<if_sid></if_sid>** tag can be used to refer to subrules within an entirely different Log Inspection Rule, you should avoid doing this because it makes the rule very difficult to review at a later time.

The list of available atomic rule conditional options are shown in the following table:

Tag	Description	Notes
match	A pattern	Any string to match against the event (log).
regex	A regular expression	Any regular expression to match against the event(log).
decoded_as	A string	Any prematched string.
srcip	A source IP address	Any IP address that is decoded as the source IP address. Use "!" to negate the IP address.
dstip	A destination IP address	Any IP address that is decoded as the destination IP address. Use "!" to negate the IP address.
srcport	A source port	Any source port (match format).
dstport	A destination port	Any destination port (match format).
user	A username	Any username that is decoded as a username.
program_name	A program name	Any program name that is decoded from the syslog process name.
hostname	A system hostname	Any hostname that is decoded as a syslog hostname.
time	A time range in the format hh:mm - hh:mm or hh:mm am - hh:mm pm	The time range that the event must fall within for the rule to trigger.
weekday	A weekday (sunday, monday, tuesday, etc.)	Day of the week that the event must fall on for the rule to trigger.
id	An ID	Any ID that is decoded from the event.
url	A URL	Any URL that is decoded from the event.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Use the **<if_sid>100125</if_sid>** tag to make this rule depend on the 100125 rule. This rule will be checked only for sshd messages that already matched the successful login rule.

```
<rule id="100127" level="10">
  <if_sid>100125</if_sid>
  <time>6 pm - 8:30 am</time>
  <description>Login outside business hours.</description>
  <group>policy_violation</group>
</rule>
```

Restrictions on the Size of the Log Entry

The following example takes the previous example and adds the **maxsize** attribute which tells the Log Inspection engine to only evaluate rules that are less than the maxsize number of characters:

```
<rule id="100127" level="10" maxsize="2000">
  <if_sid>100125</if_sid>
  <time>6 pm - 8:30 am</time>
  <description>Login outside business hours.</description>
  <group>policy_violation</group>
</rule>
```

The following table lists possible atomic rule tree-based options:

Tag	Description	Notes
if_sid	A rule ID	Adds this rule as a child rule of the rules that match the specified signature ID.
if_group	A group ID	Adds this rule as a child rule of the rules that match the specified group.
if_level	A rule level	Adds this rule as a child rule of the rules that match the specified severity level.
description	A string	A description of the rule.
info	A string	Extra information about the rule.
cve	A CVE number	Any Common Vulnerabilities and Exposures (CVE) number that you would like associated with the rule.
options	alert_by_email no_email_alert no_log	Additional rule options to indicate if the alert should generate an e-mail, alert_by_email, should not generate an email, no_email_alert, or should not log anything at all, no_log.

Composite Rules

Atomic rules examine single log entries. To correlate multiple entries, you must use composite rules. Composite rules are supposed to match the current log with those already received. Composite rules require two additional options: the **frequency** option specifies how many times an event/pattern must occur before the rule generates an alert, and the **timeframe** option tells the Log Inspection engine how far back, in seconds, it should look for previous logs. All composite rules have the following structure:

```
<rule id="100130" level="10" frequency="x" timeframe="y">
</rule>
```

For example, you could create a composite rule that creates a higher severity alert after five failed passwords within a period of 10 minutes. Using the **<if_matched_sid></if_matched_sid>** tag you can indicate which rule needs to be seen within the desired frequency and timeframe for your new rule to

© Copyright 2011 Trend Micro Inc.
All rights reserved.

create an alert. In the following example, the **frequency** attribute is set to trigger when five instances of the event are seen and the **timeframe** attribute is set to specify the time window as 600 seconds.

The **<if_matched_sid></if_matched_sid>** tag is used to define which other rule the composite rule will watch:

```
<rule id="100130" level="10" frequency="5" timeframe="600">
  <if_matched_sid>100124</if_matched_sid>
  <description>5 Failed passwords within 10 minutes</description>
</rule>
```

There are several additional tags that you can use to create more granular composite rules. These rules, as shown in the following table, allow you to specify that certain parts of the event must be the same. This allows you to tune your composite rules and reduce false positives:

Tag	Description
same_source_ip	Specifies that the source IP address must be the same.
same_dest_ip	Specifies that the destination IP address must be the same.
same_dst_port	Specifies that the destination port must be the same.
same_location	Specifies that the location (hostname or agent name) must be the same.
same_user	Specifies that the decoded username must be the same.
same_id	Specifies that the decoded id must be the same.

If you wanted your composite rule to alert on every authentication failure, instead of a specific rule ID, you could replace the **<if_matched_sid></if_matched_sid>** tag with the **<if_matched_group></if_matched_group>** tag. This allows you to specify a category, such as **authentication_failure**, to search for authentication failures across your entire infrastructure.

```
<rule id="100130" level="10" frequency="5" timeframe="600">
  <if_matched_group>authentication_failure</if_matched_group>
  <same_source_ip />
  <description>5 Failed passwords within 10 minutes</description>
</rule>
```

In addition to **<if_matched_sid></if_matched_sid>** and **<if_matched_group></if_matched_group>** tags, you can also use the **<if_matched_regex></if_matched_regex>** tag to specify a regular expression to search through logs as they are received.

```
<rule id="100130" level="10" frequency="5" timeframe="600">
  <if_matched_regex>^Failed password</if_matched_regex>
  <same_source_ip />
  <description>5 Failed passwords within 10 minutes</description>
</rule>
```

Real World Examples

Deep Security includes many default Log Inspection rules for dozens of common and popular applications. Through Security Updates, new rules are added regularly. In spite of the growing list of applications supported by Log Inspection rules, you may find the need to create a custom rule for an unsupported or custom application.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

In this section we will walk through the creation of a custom CMS (Content Management System) hosted on the Microsoft Windows Server IIS .Net platform with a Microsoft SQL Database as the data repository.

The first step is to identify the following application logging attributes:

1. Where does the application log to?
2. Which Log Inspection decoder can be used to decode the log file?
3. What is the general format of a log file message?

For our custom CMS example the answers are as follows:

1. Windows Event Viewer
2. Windows Event Log (eventlog)
3. Windows Event Log Format with the following core attributes:
    - Source: CMS
    - Category: None
    - Event: <Application Event ID>

The second step is to identify the categories of log events by application feature, then organize the categories into a hierarchy of cascading groups for inspection. Not all inspected groups need to raise events; a match can be used as a conditional statement. For each group, identify the log format attributes which the rule can use as matching criteria. This can be performed in a reverse manner by inspecting all application logs for patterns and natural groupings of log events.

For example, the CMS application supports the following functional features which we will create log inspection rules for:

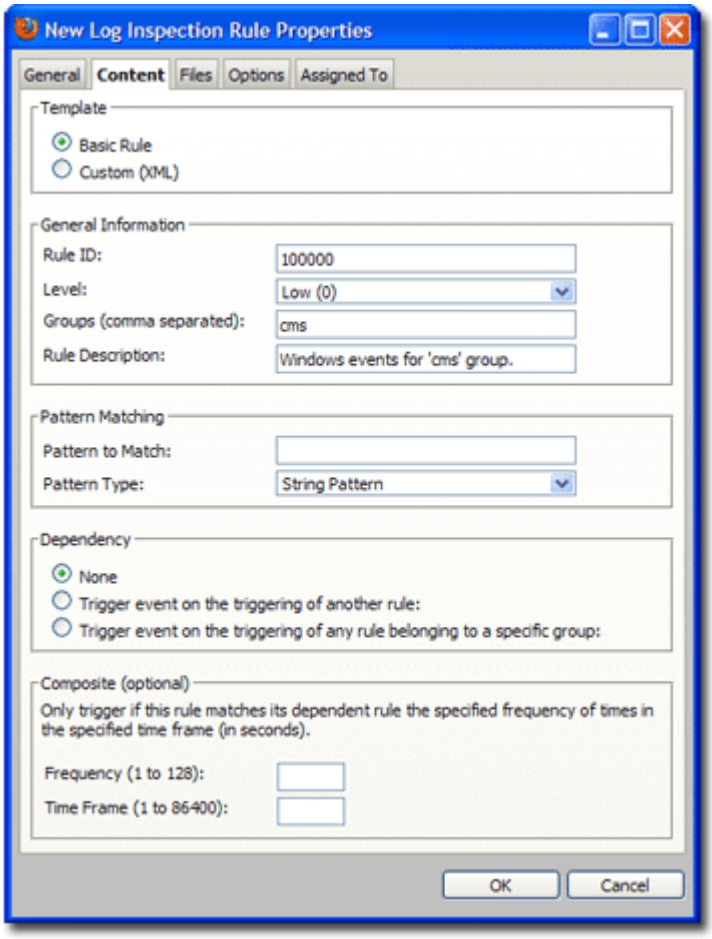
- CMS Application Log (Source: CMS)
    - Authentication (Event: 100 to 119)
        - User Login successful (Event: 100)
        - User Login unsuccessful (Event: 101)
        - Administrator Login successful (Event: 105)
        - Administrator Login unsuccessful (Event: 106)
    - General Errors (Type: Error)
        - Database error (Event: 200 to 205)
        - Runtime error (Event: 206-249)
    - Application Audit (Type: Information)
        - Content
            - New content added (Event: 450 to 459)
            - Existing content modified (Event: 460 to 469)
            - Existing content deleted (Event: 470 to 479)
        - Administration
            - User
                - New User created (Event: 445 to 446)
                - Existing User deleted (Event: 447 to 449)

This structure will provide you with a good basis for rule creation. Now to create a new Log Inspection rule in Deep Security Manager.

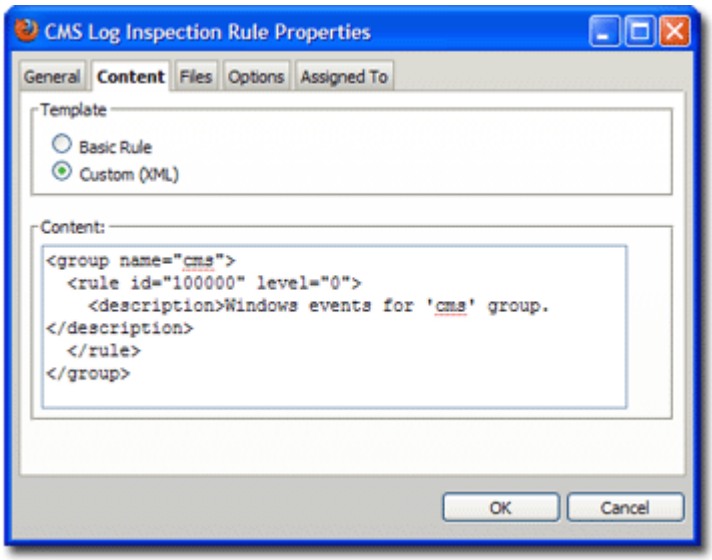
To create the new CMS Log Inspection Rule:

1. In Deep Security Manager, go to **Log Inspection > Log Inspection Rules** and click **New** to display the **New Log Inspection Rule Properties** window.
2. Give the new rule a Name and a Description, and then click the **Content** tab.
3. The quickest way to create a new custom rule is to start with a basic rule template. Select the **Basic Rule** radio button.
4. The **Rule ID** field will be automatically populated with an unused ID number between 100,000 and 199,000, the IDs reserved for custom rules.
5. Set the **Level** setting to **Low (0)**.
6. Give the rule an appropriate Group name. In this case, "cms".
7. Provide a short rule description.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

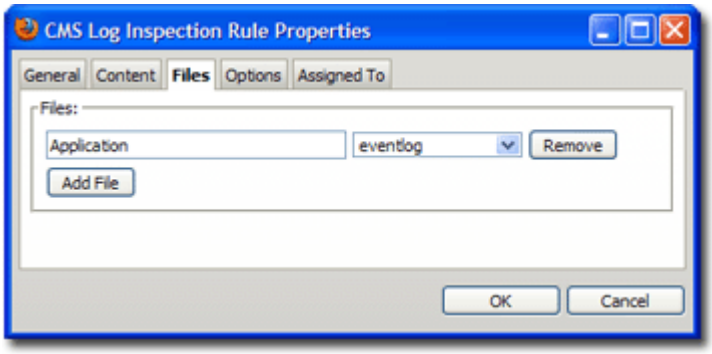


8. Now select the **Custom (XML)** option. The information you have entered will be used to generate the XML for your rule.



9. Next, click the **Files** tab and click the **Add File** button to add any application log files and log types which the rule will be applied to. In this case, "Application", and "eventlog" as the file type.

© Copyright 2011 Trend Micro Inc.
All rights reserved.



Eventlog is a unique file type in Deep Security because the location and filename of the log files don't have to be specified. Instead, it is sufficient to type the log name as it is displayed in the Windows Event Viewer. Other log names for the eventlog file type might be "Security", "System", "Internet Explorer", or any other section listed in the Windows Event Viewer. Other file types will require the log file's location and filename. (*C/C++ strftime()* conversion specifiers are available for matching on filenames. See the table below for a list of some of the more useful ones.)

10. Click **OK** to save the basic rule.
11. Working with the basic rule Custom (XML) created, we can begin adding new rules to the group based on the log groupings identified previously. We will set the base rule criteria to the initial rule. In the following example, the CMS base rule has identified Windows Event Logs with a Source attribute of "CMS":

```
<group name="cms">
  <rule id="100000"  level="0">
    <category>windows</category>
    <extra_data>^CMS</extra_data>
    <description>Windows events from  source 'CMS' group
messages.</description>
  </rule>
```

12. Now we build up subsequent rules from the identified log groups. The following example identifies the authentication and login success and failure and logs by Event IDs.

```
<rule id="100001"  level="0">
    <if_sid>100000</if_sid>
    <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
    <group>authentication</group>
    <description>CMS Authentication event.</description>
  </rule>

  <rule id="100002"  level="0">
    <if_group>authentication</if_group>
    <id>100</id>
    <description>CMS User Login success event.</description>
  </rule>

  <rule id="100003"  level="4">
    <if_group>authentication</if_group>
    <id>101</id>
```

© Copyright 2011 Trend Micro Inc.
All rights reserved.

```
    <group>authentication_failure</group>
    <description>CMS User Login failure event.</description>
  </rule>

  <rule id="100004"  level="0">
    <if_group>authentication</if_group>
    <id>105</id>
    <description>CMS Administrator Login success event.</description>
  </rule>

  <rule id="100005"  level="4">
    <if_group>authentication</if_group>
    <id>106</id>
    <group>authentication_failure</group>
    <description>CMS Administrator Login failure event.</description>
  </rule>
```

13. Now we add any composite or correlation rules using the established rules. The follow example shows a high severity composite rule which is applies to instances where the repeated login failures have occurred 5 times within a 10 second time period:

```
  <rule id="100006" level="10"  frequency="5" timeframe="10">
    <if_matched_group>authentication_failure</if_matched_group>
    <description>CMS Repeated Authentication Login failure
event.</description>
  </rule>
```

14. Review all rules for appropriate severity levels. For example, error logs should have a severity of level 5 or higher. Informational rules would have a lower severity.

15. Finally, open the newly created rule, click the **Configuration** tab and copy your custom rule XML into the rule field. Click **Apply** or **OK** to save the change.

Once the rule is assigned to a Security Profile or computer, the Log Inspection engine should begin inspecting the designated log file immediately.

The complete Custom CMS Log Inspection Rule:

```
<group  name="cms">

   <rule id="100000"  level="0">
    <category>windows</category>
    <extra_data>^CMS</extra_data>
    <description>Windows events from source 'CMS' group
messages.</description>
   </rule>

   <rule id="100001"  level="0">
    <if_sid>100000</if_sid>
    <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
    <group>authentication</group>
```

© Copyright 2011 Trend Micro Inc.
All rights reserved.

```
    <description>CMS Authentication event.</description>
  </rule>

  <rule id="100002"  level="0">
    <if_group>authentication</if_group>
    <id>100</id>
    <description>CMS User Login success event.</description>
  </rule>

  <rule id="100003"  level="4">
    <if_group>authentication</if_group>
    <id>101</id>
    <group>authentication_failure</group>
    <description>CMS User Login failure event.</description>
  </rule>

  <rule id="100004"  level="0">
    <if_group>authentication</if_group>
    <id>105</id>
    <description>CMS Administrator Login success event.</description>
  </rule>

  <rule id="100005"  level="4">
    <if_group>authentication</if_group>
    <id>106</id>
    <group>authentication_failure</group>
    <description>CMS Administrator Login failure event.</description>
  </rule>

  <rule id="100006"  level="10" frequency="5" timeframe="10">
    <if_matched_group>authentication_failure</if_matched_group>
    <description>CMS Repeated Authentication Login failure
event.</description>
  </rule>

  <rule id="100007"  level="5">
    <if_sid>100000</if_sid>
    <status>^ERROR</status>
    <description>CMS General error event.</description>
    <group>cms_error</group>
  </rule>

  <rule id="100008"  level="10">
    <if_group>cms_error</if_group>
    <id>^200|^201|^202|^203|^204|^205</id>
    <description>CMS Database error event.</description>
```

© Copyright 2011 Trend Micro Inc.
All rights reserved.

```
    </rule>

    <rule id="100009"  level="10">
     <if_group>cms_error</if_group>

<id>^206|^207|^208|^209|^230|^231|^232|^233|^234|^235|^236|^237|^238|^23
9^|240|^241|^242|^243|^244|^245|^246|^247|^248|^249</id>
     <description>CMS Runtime error event.</description>
    </rule>

    <rule id="100010"  level="0">
     <if_sid>100000</if_sid>
     <status>^INFORMATION</status>
     <description>CMS General informational event.</description>
     <group>cms_information</group>
    </rule>

    <rule id="100011"  level="5">
     <if_group>cms_information</if_group>
     <id>^450|^451|^452|^453|^454|^455|^456|^457|^458|^459</id>
     <description>CMS New Content added event.</description>
    </rule>

    <rule id="100012"  level="5">
     <if_group>cms_information</if_group>
     <id>^460|^461|^462|^463|^464|^465|^466|^467|^468|^469</id>
     <description>CMS Existing Content modified event.</description>
    </rule>

    <rule id="100013"  level="5">
     <if_group>cms_information</if_group>
     <id>^470|^471|^472|^473|^474|^475|^476|^477|^478|^479</id>
     <description>CMS Existing Content deleted event.</description>
    </rule>

    <rule id="100014"  level="5">
     <if_group>cms_information</if_group>
     <id>^445|^446</id>
     <description>CMS User created event.</description>
    </rule>

    <rule id="100015"  level="5">
     <if_group>cms_information</if_group>
     <id>^447|449</id>
     <description>CMS User deleted event.</description>
    </rule>
```

© Copyright 2011 Trend Micro Inc.
All rights reserved.

```
</group>
```

Log Inspection Rule Severity Levels and their Recommended Use

Level	Description	Notes
Level 0	Ignored, no action taken	Primarily used to avoid false positives. These rules are scanned before all the others and include events with no security relevance.
Level 1	no predefined use	
Level 2	System low priority notification	System notification or status messages that have no security relevance.
Level 3	Successful/authorized events	Successful login attempts, firewall allow events, etc.
Level 4	System low priority errors	Errors related to bad configurations or unused devices/applications. They have no security relevance and are usually caused by default installations or software testing.
Level 5	User-generated errors	Missed passwords, denied actions, etc. These messages typically have no security relevance.
Level 6	Low relevance attacks	Indicate a worm or a virus that provide no threat to the system such as a Windows worm attacking a Linux server. They also include frequently triggered IDS events and common error events.
Level 7	no predefined use	
Level 8	no predefined use	
Level 9	Error from invalid source	Include attempts to login as an unknown user or from an invalid source. The message might have security relevance especially if repeated. They also include errors regarding the **admin** or **root** account.
Level 10	Multiple user generated errors	Include multiple bad passwords, multiple failed logins, etc. They might indicate an attack, or it might be just that a user forgot his or her credentials.
Level 11	no predefined use	
Level 12	High-importance event	Include error or warning messages from the system, kernel, etc. They might indicate an attack against a specific application.
Level 13	Unusual error (high importance)	Common attack patterns such as a buffer overflow attempt, a larger than normal syslog message, or a larger than normal URL string.
Level 14	High importance security event	Typically the result of the correlation of multiple attack rules and indicative of an attack.
Level 15	Attack Successful	Very small chance of false positive. Immediate attention is necessary.

strftime() Conversion Specifiers

Specifier	Description
%a	Abbreviated weekday name (e.g., Thu)
%A	Full weekday name (e.g., Thursday)
%b	Abbreviated month name (e.g., Aug)

© Copyright 2011 Trend Micro Inc.
All rights reserved.

%B	Full month name (e.g., August)
%c	Date and time representation (e.g., Thu Sep 22 12:23:45 2007)
%d	Day of the month (01–31) (e.g., 20)
%H	Hour in 24 h format (00–23) (e.g., 13)
%I	Hour in 12 h format (01–12) (e.g., 02)
%j	Day of the year (001–366) (e.g., 235)
%m	Month as a decimal number (01–12) (e.g., 02)
%M	Minute (00–59) (e.g., 12)
%p	AM or PM designation (e.g., AM)
%S	Second (00–61) (e.g., 55)
%U	Week number with the first Sunday as the first day of week one (00–53) (e.g., 52)
%w	Weekday as a decimal number with Sunday as 0 (0–6) (e.g., 2)
%W	Week number with the first Monday as the first day of week one (00–53) (e.g., 21)
%x	Date representation (e.g., 02/24/79)
%X	Time representation (e.g., 04:12:51)
%y	Year, last two digits (00–99) (e.g., 76)
%Y	Year (e.g., 2008)
%Z	Time zone name or abbreviation (e.g., EST)
%%	A % sign (e.g., %)

More information can be found at the following Web sites:

- http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vclib/html/_crt_strftime.2c_.wcsftime.asp
- www.php.net/strftime
- www.cplusplus.com/reference/clibrary/ctime/strftime.html

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Creating and Applying New Firewall Rules

Firewall Rules are composed of six basic elements:

- **Action:** whether the Agent/Appliance will allow packets matching the rule's criteria through regardless of any other rules that would block them ("force allow"); block packets matching the rule's criteria ("deny"); exclusively allow only packets matching the rule's criteria and block all others ("Allow"); or log packets matching the rule's criteria and let them pass ("log only"). Within a priority level (see next item), rules are applied in this order:
    1. "bypass"
    2. "force allow"
    3. "deny"
    4. "allow"
    5. "log only"
- **Priority:** Firewall Rules can have a priority of 0 (lowest) to 4 (highest). High priority rules are applied first.
- **Packet Direction:** whether the packet is incoming or outgoing.
- **Packet Source :** all the information that describes the packet's source (frame type, protocol, IPs, ports, flags, etc.)
- **Packet Destination :** all the information that describes the packet's destination (frame type, protocol, IPs, ports, flags, etc.)
- **Specific Flags:** which particular to flags have to be set for the rule to trigger. (Flags will vary depending on protocol.)

To create a new Firewall Rule:

1. Go to the **Firewall Rules** screen and click **New** in the toolbar.
2. Type a name and description for your new Firewall Rule.
3. Select a rule action, priority, and packet direction from the drop-down lists.
4. Define the criteria that this rule will look for in the packets' control information. (As well as inclusive criteria, you can define exclusive criteria by checking the "Not" checkbox at the right of each option.)
5. Click the **Options** tab and select whether you want the rule to only be active during certain scheduled periods. Specify whether you want this rule to trigger an alert when it is triggered.
6. Click **OK** to close the **New Firewall Rule** Properties Window.

Now you have to assign the new Firewall Rule to a computer. The best way to manage the application of Firewall Rules to computers is by way of Security Profiles. Having a Security Profile called "Developer Laptop", for example, allows you to create a set of Firewall Rules all designed for the particular environment "developer laptops" operate in. You can then assign them all to the "Developer Laptop" Security Profile, and then assign that Security Profile to that collection of computers. Anytime you need to create and assign a new Firewall Rule to your "developer laptops", you just assign it to the Security Profile, and all "Developer Laptop" computers will be updated with the new Firewall Rule.

To include a new Firewall Rule in a Security Profile:

1. Go to the **Security Profiles** screen and double-click the Security Profile to which you want to assign a new rule. This will open the Profile's **Details** window.
2. Click the **Firewall Rules** tab.
3. Find your new Firewall Rule in the list and put a check in its checkbox.
4. Click **OK**.

If the "Automatically update all affected computers after changing any aspect of the Deep Security System." option is enabled on the **Computers** tab in the **System > System Settings** screen, all computers to which that Security Profile has been assigned will be updated with the new rule.

Optionally, you can assign a new Firewall Rule directly to a computer:

© Copyright 2011 Trend Micro Inc.
All rights reserved.

1. Go to the **Computers** screen and double click the computer to which you want to assign the new rule.
2. Click the **Firewall Rules** tab.
3. Find your new Firewall Rule in the list.
4. Put a check in its checkbox and click the **OK** button.

As before, if the "Automatically update all affected computers after changing any aspect of the Deep Security System." option is enabled on the **Computers** tab in the **System > System Settings** screen, all computers to which that Security Profile has been assigned will be updated with the new rule.

Note that if you apply other settings to a computer (for example, adding additional Firewall Rules, or modifying stateful configuration settings), an asterisk will appear next to the name of the Security Profile (in the **Security Profile** column in the **Computers** screen) indicating that the default settings have been changed.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

DPI Events

Event	Notes
Base 64 Decoding Error	Packet content that was expected to be encoded in Base64 format was not encoded correctly.
Client Attempted to Rollback	A client attempted to rollback to an earlier version of the SSL protocol than that which was specified in the ClientHello message.
Corrupted Deflate/GZIP Content	Corrupted Deflate/GZIP Content
Deflate/GZIP Checksum Error	Deflate/GZIP Checksum Error.
Double Decoding Exploit	Double decoding exploit attempt (%25xx, %25%xxd, etc).
Edit Too Large	Editing attempted to increase the size of the region above the maximum allowed size (8188 bytes).
Error Decrypting Pre-master Key	Unable to un-wrap the pre-master secret from the ClientKeyExchange message.
Error Generating Master Key(s)	Unable to derive the cryptographic keys, Mac secrets, and initialization vectors from the master secret.
Error Generating Pre-Master Request	An error occurred when trying to queue the pre-master secret for decryption.
Handshake Message (not ready)	The SSL state engine has encountered a handshake message after the handshake has been negotiated.
Illegal Character in URI	Illegal character used in uri.
Incomplete Deflate/GZIP Content	Corrupted deflate/gzip content.
Incomplete UTF8 Sequence	URI ended in middle of utf8 sequence.
Int Min/Max/Choice Constraint Failure	A protocol decoding rule decoded data that did not meet the protocol content constraints.
Internal Error	The protocol decoding engine detected an internal corruption while processing a loop or nested type.
Invalid Hex Encoding	%nn where nn are not hex digits.
Invalid Lexical Instruction	An internal error occurred causing the protocol decoding stack to become corrupt and halt processing for the connection.
Invalid Parameters In Handshake	An invalid or unreasonable value was encountered while trying to decode the handshake protocol.
Invalid Traversal	Tried to use "../../" above root.
Invalid Use of Character	use of disabled char
Invalid UTF8 encoding	Invalid/non-canonical encoding attempt.
Key Exchange Error	The server is attempting to establish an SSL session with temporarily generated key.
Key Too Large	The master secret keys are larger than specified by the protocol identifier.
Max Matches in Packet Exceeded	There are more than 2048 positions in the packet with pattern match occurrences. An error is returned at this limit and the connection is dropped because this usually indicates a garbage or evasive packet.
Maximum Edits Exceeded	The maximum number of edits (32) in a single region of a packet was exceeded.
Memory Allocation Error	The packet could not be processed properly because resources were exhausted. This can be because too many

© Copyright 2011 Trend Micro Inc.
All rights reserved.

	concurrent connections require buffering (max 2048) or matching resources (max 128) at the same time or because of excessive matches in a single IP packet (max 2048) or simply because the system is out of memory.
Out Of Order Handshake Message	A well formatted handshake message has been encountered out of sequence.
Packet Read Error	Low level problem reading packet data.
Record Layer Message	The SSL state engine has encountered an SSL record before initialization of the session.
Region Too Big	A region (edit region, uri etc) exceeded the maximum allowed buffering size (7570 bytes) without being closed. This is usually because the data does not conform to the protocol.
Renewal Error	An SSL session was being requested with a cached session key that could not be located.
Runtime Error.	Runtime error.
Search Limit Reached	A protocol decoding rule defined a limit for a search or pdu object but the object was not found before the limit was reached.
Stack Depth	A rule programming error attempted to cause recursion or use to many nested procedure calls.
Type Nesting Too Deep	A protocol decoding rule encountered a type definition and packet content that caused the maximum type nesting depth (16) to be exceeded.
Unsupported Cipher	An unknown or unsupported Cipher Suite has been requested.
Unsupported Deflate/GZIP Dictionary	Unsupported Deflate/GZIP Dictionary.
Unsupported GZIP Header Format/Method	Unsupported GZIP Header Format/Method.
Unsupported SSL Version	A client attempted to negotiate an SSL V2 session.
URI Path Depth Exceeded	too many "/" separators, max 100 path depth.
URI Path Length Too Long	path length is greater than 512 characters.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Disabling Diffie-Hellman in Apache

An Apache Web server may use the Diffie-Hellman (DH) public key cryptography protocol as the "Key Exchange Algorithm" and "Authentication Method". This protocol is not supported by the Deep Security Agent/Appliance and must be disabled on an Apache Web server for SSL filtering to work.

The "Key Exchange Algorithm" and "Authentication Method" parameters are the first two fields of the "`SSLCipherSuite`" variable present in the `httpd-ssl.conf` file. To instruct Apache to not use Diffie-Hellman, "`!ADH`" must be added to these fields.

The following example shows the syntax required to disable DH key exchange and authentication methods in Apache:

```
SSLCipherSuite
!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
```

Note that only the first two fields are of concern with regards to disabling ADH. The "`!`" tells Apache to "Not" use ADH.

The config files may be located in different places depending on your Apache build. For example:

- **Default installation on RHEL4:** `/etc/httpd/conf.d/ssl.conf`
- **Apache 2.2.2:** `/usr/local/apache2/conf/extra/httpd-ssl.conf`

References

For more information, visit the Apache Documentation of `SSLCipherSuite` at http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Encrypting DSM to DB Communication

Communication between the Deep Security Manager and the database is not encrypted by default. This is for performance reasons and because the channel between the Manager and the database may already be secure (either they are running on the same computer or they are connected by crossover cable, a private network segment, or tunneling via IPSec).

However, if the communication channel between the Deep Security Manager and the database is not secure, you should encrypt the communications between them. Do this by editing the `dsm.properties` file located in `\Deep Security Manager\webclient\webapps\ROOT\WEB-INF\`

If you are running the Deep Security Manager in multi-node mode, these changes must be made on each node.

MS SQL Server

Add the following line to `dsm.properties`:

```
database.SqlServer.ssl=require
```

Save and close the file. Stop and restart the Deep Security Manager service.

Oracle Database

Add the following lines to `dsm.properties`:

```
database.Oracle.oracle.net.encryption_types_client=(3DES168)
database.Oracle.oracle.net.encryption_client=REQUIRED
database.Oracle.oracle.net.crypto_checksum_types_client=(MD5)
database.Oracle.oracle.net.crypto_checksum_client=REQUIRED
```

Save and close the file. Stop and restart the Deep Security Manager service.

Note that Oracle Database must be configured to accept encrypted communication. Consult your Oracle Database documentation for instructions.

Running an Agent on the Database Server

Encryption should be enabled if you are using an Agent to protect the database. When you carry out a Security Update, the Deep Security Manager stores new DPI Rules in the database. The rule names themselves will almost certainly generate false positives as they get parsed by the Agent if the data is not encrypted.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Event Tagging

With the introduction of the Integrity Monitoring and Log Inspection features, an increasing number of events get forwarded to the Deep Security Management console. This has created the need for new tools to automate the management of these events.

Event Tagging is a new feature that allows administrators to manually tag events with predefined labels ("attack", "suspicious", "patch", "acceptable change", "false positive", "high priority", etc.) and the ability to define custom labels ("Assigned to Tom for review", etc.).

In addition to the manual tagging of events, automated event tagging can be accomplished via the use of a "Reference Computer" which is particularly useful for managing Integrity Monitoring events. For example, a planned rollout of a patch can be applied to the reference computer, the events associated with the application of the patch can be tagged as "Patch X", similar events raised on other systems can automatically be deemed to be "acceptable changes" and suppressed to reduce the number of events subjected to scrutiny by an administrator.

Event tagging enables specialized views of events, dashboards, and reports and can be applied to a single event, similar events, or even to all future similar events.

Tagging Events

The following procedures apply to all types of Events (Firewall, DPI, Log Inspection, System, etc.).

To tag a single Event:

1. Right-click on the event in the **Events** list and select **Add Tag(s)...**.
2. Type a name for the tag. (Deep Security Manager will suggest matching names of existing tags as you type.)
3. Select **1 Selected System Event**. (You can select multiple events at once from the Events list, in which case the number of selected events will be displayed.) Click **Next**.

Depending on the type of event (Firewall, DPI, Integrity Monitoring, etc.), you may be able to select **Display Advanced Settings**. Advanced settings will include further criteria for refining the selection of the events you want to tag.

4. Enter some optional comments and click **Finish**.

Looking at the Events list, you can see that the Event has now been tagged.

To tag multiple similar Events:

1. Right click on a representative event from the Events list and select **Add tag(s)...**.
2. Type a name for the tag. (Deep Security Manager will suggest matching names of existing tags as you type.)
3. Select **Also apply to similar Events**.

Depending on the type of event (Firewall, DPI, Integrity Monitoring, etc.), you may be able to select **Display Advanced Settings**. Advanced settings will include further criteria for refining the selection of the events you want to tag.

Select **Include Advanced Options**, if available. Click **Next**.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

4. If you were able to select **Include Advanced Options** you will see a screen that allows you to narrow your event selection. For example, you could look for similar events only on a specific computer, or group of computers. If this is the case, make your selections and click **Next**.
5. Select which attributes will be examined to determine whether Events are similar or not. For the most part, the attribute options are the same as the information displayed in the columns of the Events list screens (Source IP, Reason, Severity, etc.). When you have selected which attributes to include in the Event selection process, click **Next**.
6. Select existing **Log Inspection Events** to identify and tag currently existing events, and select **Update Now** to initiate the search for all similar Events (rather than have the search run in the background at a low priority).

Notice the **Save Auto-Tag Rule** option. The selection criteria you have specified can be saved so that you can apply them again at a future date when new events have accumulated. Saved auto-tag rules can be found in the **System > Tags** screen.

7. Review the Summary of your Event selection criteria and click **Finish**.

Looking at the Events list, you can see that your original Event and all similar Events have been tagged.

To tag multiple similar Events as well as future similar Events:

The procedure for tagging multiple similar as well as future Events is the same as above except for step 3, where you also select **New [Event Type] Events** (where "[Event Type]" depends on the type of Events you are tagging (Firewall, DPI, Integrity Monitoring, etc.)). Selecting **New [Event Type] Events** causes the Deep Security Manager to scan its database every five seconds (or more) for new Events and tag the appropriate ones.

Tagging only occurs after Events have been retrieved from the Agents/Appliances to the Deep Security Manager's database.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Firewall Events

Event	Notes
CE Flags	The CWR or ECE flags were set and the stateful configuration specifies that these packets should be denied.
Dropped Retransmit	Dropped Retransmit.
First Fragment Too Small	A fragmented packet was encountered, the size of the fragment was less than the size of a TCP packet (no data).
Fragment Offset Too Small	The offsets(s) specified in a fragmented packet sequence is less than the size of a valid datagram.
Fragment Out Of Bounds	The offsets(s) specified in a fragmented packet sequence is outside the range of the maximum size of a datagram.
Fragmented	A fragmented packet was encountered with deny fragmented packets disallowed enabled.
Internal Driver Error	Insufficient resources.
Internal States Error	Internal TCP stateful error.
Invalid ACK	A packet with an invalid acknowledgement number was encountered.
Invalid Adapter Configuration	An invalid adapter configuration has been received.
Invalid Data Offset	Invalid data offset parameter.
Invalid Flags	Flag(s) set in packet were invalid. This could be due to a flag that does not make sense within the context of a current connection (if any), or due to a nonsensical combination of flags. (Stateful Configuration must be **On** for connection context to be assessed.)
Invalid IP	Packet's source IP was not valid.
Invalid IP Datagram Length	The length of the IP datagram is less than the length specified in the IP header.
Invalid Port Command	An invalid FTP port command was encountered in the FTP control channel data stream.
Invalid Sequence	A packet with an invalid sequence number or out-of-window data size was encountered.
Invalid IP Header Length	An invalid IP header length (< 5*4 = 20) was set in the IP header.
IP Version Unknown	An IP packet other than IPv4 or IPv6 was encountered.
IPv6 Packet	An IPv6 Packet was encountered, and IPv6 blocking is enabled.
Max Incoming Connections	The number of incoming connections has exceeded the maximum number of connections allowed.
Max Outgoing Connections	The number of outgoing connections has exceeded the maximum number of connections allowed.
Max SYN Sent	The number of half open connections from a single computer exceeds that specified in the stateful configuration.
Maximum ACK Retransmit	This retransmitted ACK packet exceeds the ACK storm protection threshold.
Null IP	a NULL (0.0.0.0) IP is not allowed by the present firewall configuration
Out Of Allowed Policy	The packet does not meet any of the Allow or Force Allow rules and so is implicitly denied.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Out Of Connection	A packet was received that was not associated with an existing connection.
Overlapping Fragment	This packet fragment overlaps a previously sent fragment.
Packet on Closed Connection	A packet was received belonging to a connection already closed.
Same Source and Destination IP	Source and destination IPs were identical.
SYN Cookie Error	The SYN cookies protection mechanism encountered an error.
Unknown IP Version	Unrecognized IP version.
Unreadable Ethernet Header	Data contained in this Ethernet frame is smaller than the Ethernet header.
Unreadable IPv4 Header	The packet contains an unreadable IPv4 header.
Unreadable Protocol Header	The packet contains an unreadable TCP, UDP or ICMP header.
Unsolicited ICMP	ICMP stateful has been enabled (in stateful configuration) and an unsolicited packet that does not match any Force Allow rules was received.
Unsolicited UDP	Incoming UDP packets that were not solicited by the computer are rejected.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Firewall Rule Sequence

Packets arriving at a computer running an Agent/Appliance get processed first by Firewall Rules, then the Stateful Configuration conditions, and finally by the DPI Rules.

This is the order in which Firewall Rules are applied (incoming and outgoing):

1. Firewall Rules with priority 4 (highest)
    1. **Bypass**
    2. **Log Only** (**Log Only** rules can only be assigned a priority of **4 (highest)**)
    3. **Force Allow**
    4. **Deny**
2. Firewall Rules with priority 3 (high)
    1. **Bypass**
    2. **Force Allow**
    3. **Deny**
3. Firewall Rules with priority 2 (normal)
    1. **Bypass**
    2. **Force Allow**
    3. **Deny**
4. Firewall Rules with priority 1 (low)
    1. **Bypass**
    2. **Force Allow**
    3. **Deny**
5. Firewall Rules with priority 0 (lowest)
    1. **Bypass**
    2. **Force Allow**
    3. **Deny**
    4. **Allow** (Note that an **Allow** rule can only be assigned a priority of **0 (lowest)**)

Within the same priority context, a **deny** rule will override an **allow** rule, and a **force allow** rule will override a **deny** rule. By using the rule priorities system, a higher priority **deny** rule can be made to override a lower priority **force allow** rule.

Consider the example of a DNS server policy that makes use of a **force allow** rule to allow all incoming DNS queries over TCP/UDP port 53. Creating a **deny** rule with a higher priority than the **force allow** rule lets you specify a particular range of IP addresses that must be prohibited from accessing the same public server.

Priority-based rule sets allow you set the order in which the rules are applied. If a **deny** rule is set with the highest priority, and there are no **force allow** rules with the same priority, then any packet matching the **deny** rule is automatically dropped and the remaining rules are ignored. Conversely, if a **force allow** rule with the highest priority flag set exists, any incoming packets matching the **force allow** rule will be automatically allowed through without being checked against any other rules.

A Note on Logging

Bypass Rules will never generate a log entry. This is not configurable.

Log-only rules will only generate a log entry if the packet in question is not subsequently stopped by either:

- a **deny** rule, or
- an **allow** rule that excludes it.

If the packet is stopped by one of those two rules, those rules will generate the log entry and not the **log-only** rule. If no subsequent rules stop the packet, the **log-only** rule will generate an entry.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

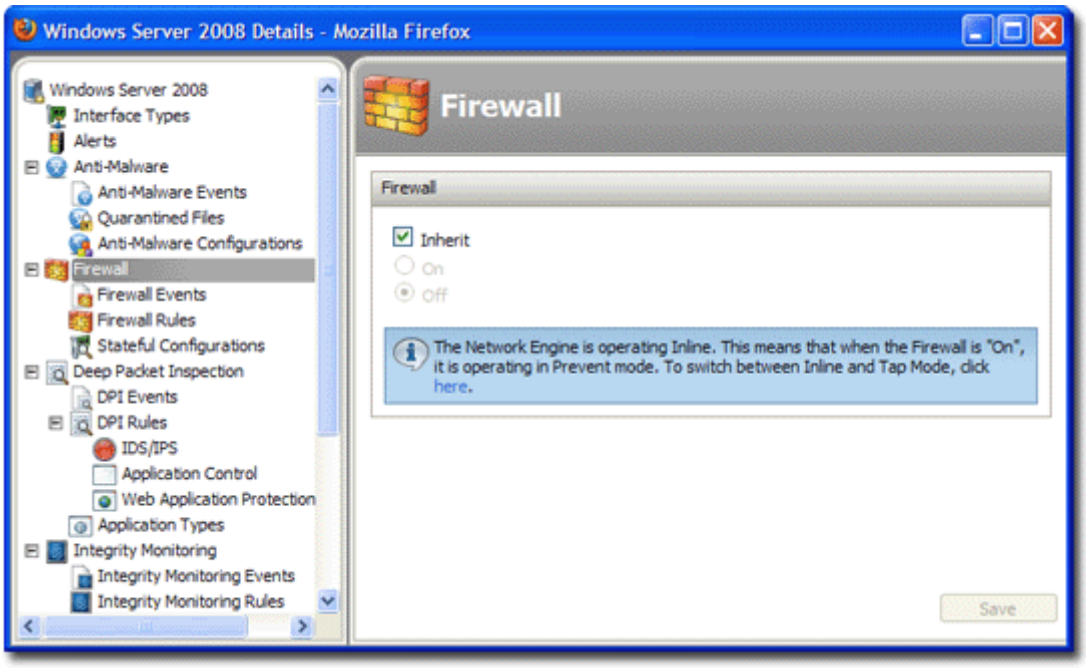
Inheritance and Overrides

Settings

Global settings can be overridden by settings at the Security Profile or computer level. For example, the Firewall can be turned off globally by going to the Firewall screen in the main Deep Security Manager window and setting "Firewall" to off.

By default, lower levels in the hierarchy inherit their settings from the level above them. Therefore, if you turn off the Firewall at the Global level, it will be turned off in all Security Profiles and computers that are set to "Inherit".

© Copyright 2011 Trend Micro Inc.
All rights reserved.

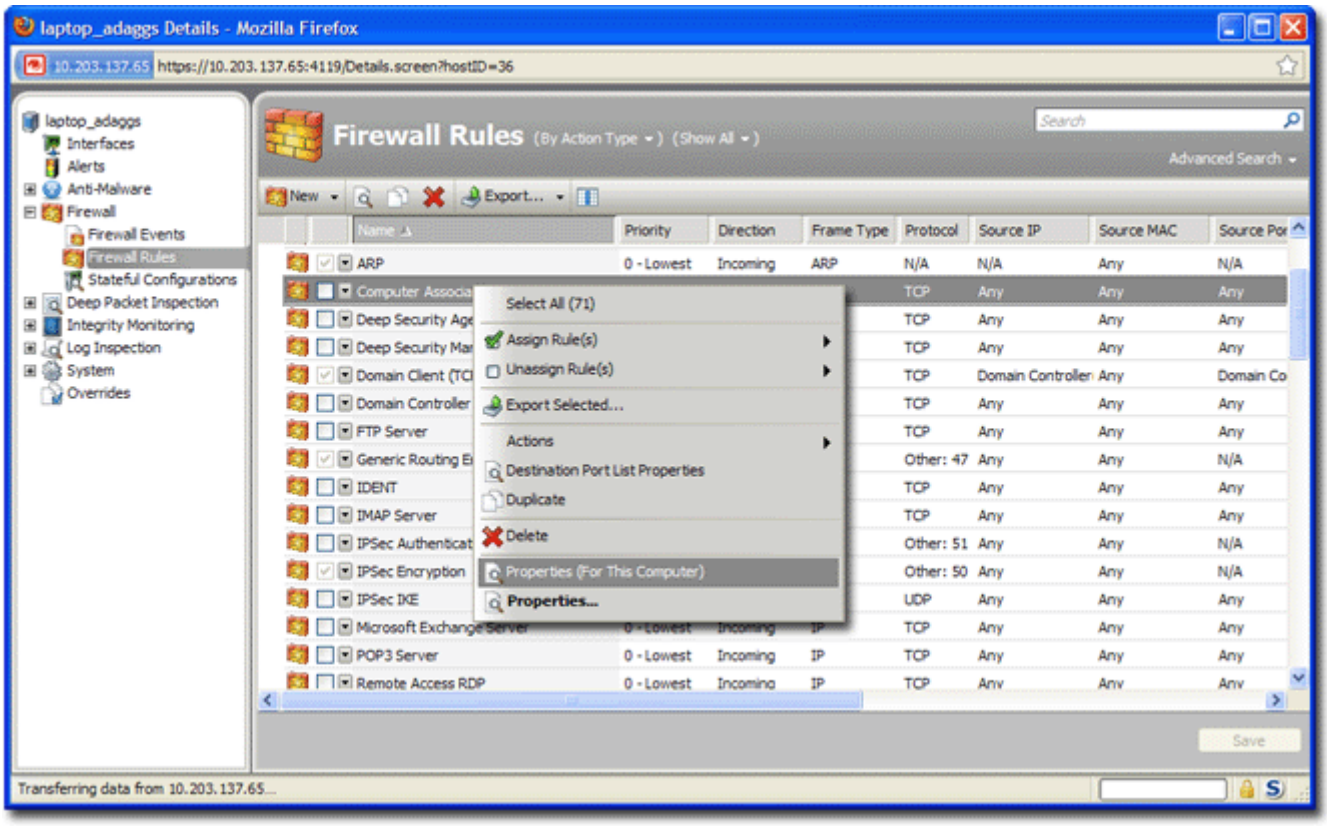


Other Properties

Elements like Firewall Rules and DPI Rules can have some of their properties changed for specific computers. For example, let's say you have a Firewall Rule called FirewallRuleAlpha and among its properties is the fact that it operates on incoming port 12345 because the application you have designed the Firewall Rule for usually operates on that port.

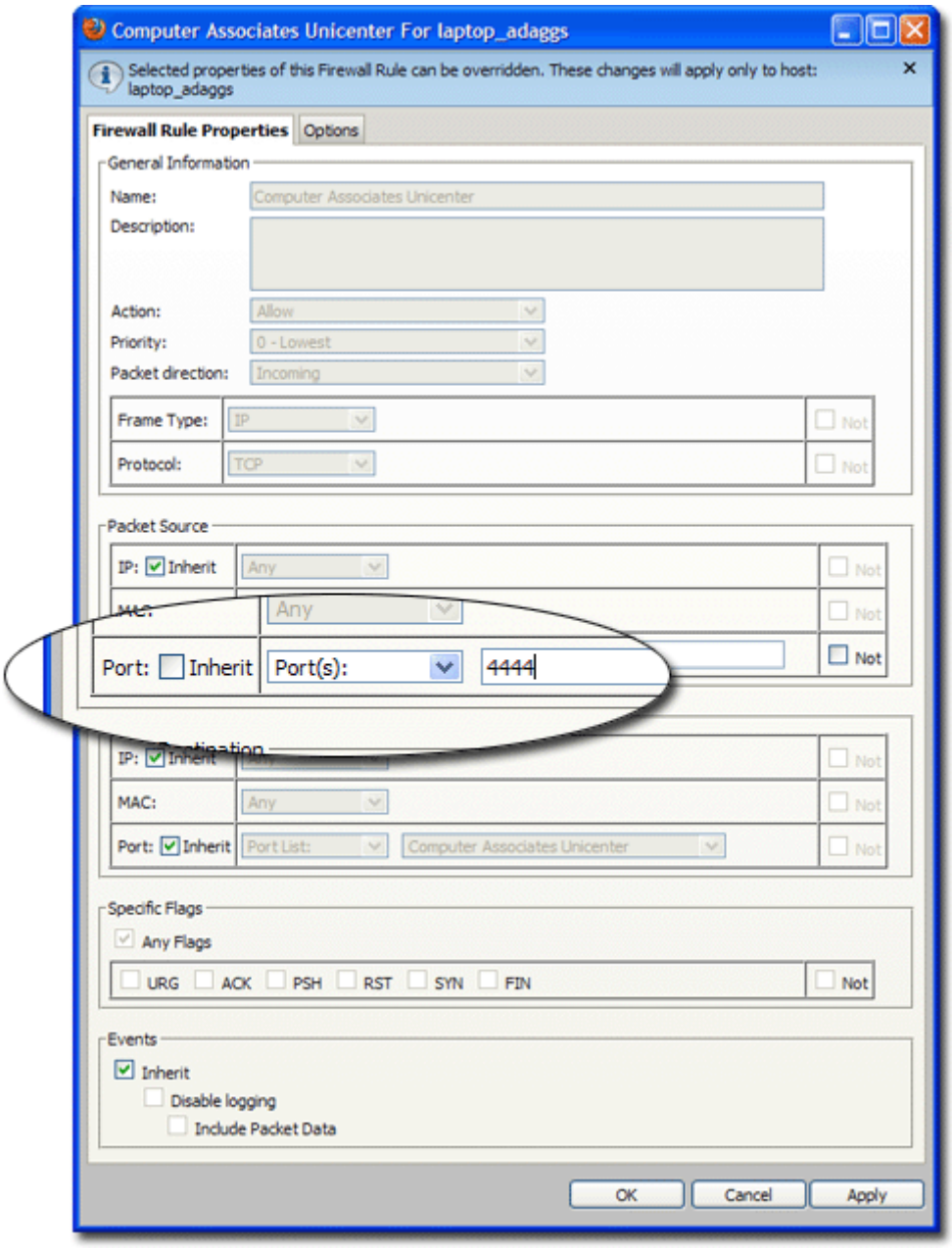
But let's say you have one particular computer where that application operates on port 44444. Instead of writing a new Firewall Rule for this computer, we can simply open the computer's **Details** window, go to **Firewall Rules**, find the Firewall Rule in the list, right-click it and select "Properties (For This Computer)".

© Copyright 2011 Trend Micro Inc.
All rights reserved.



In the **Properties** window for this Firewall Rule you will now see that many of the properties have a checkbox called "Inherit" next to them. This means that the setting is inherited from the level above it in the inheritance hierarchy (either from a Security Profile or the Global list). Clearing "Inherited" next to "Port:" and changing it to 44444 means that this Firewall Rule *on this computer only* will now operate on port 44444.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

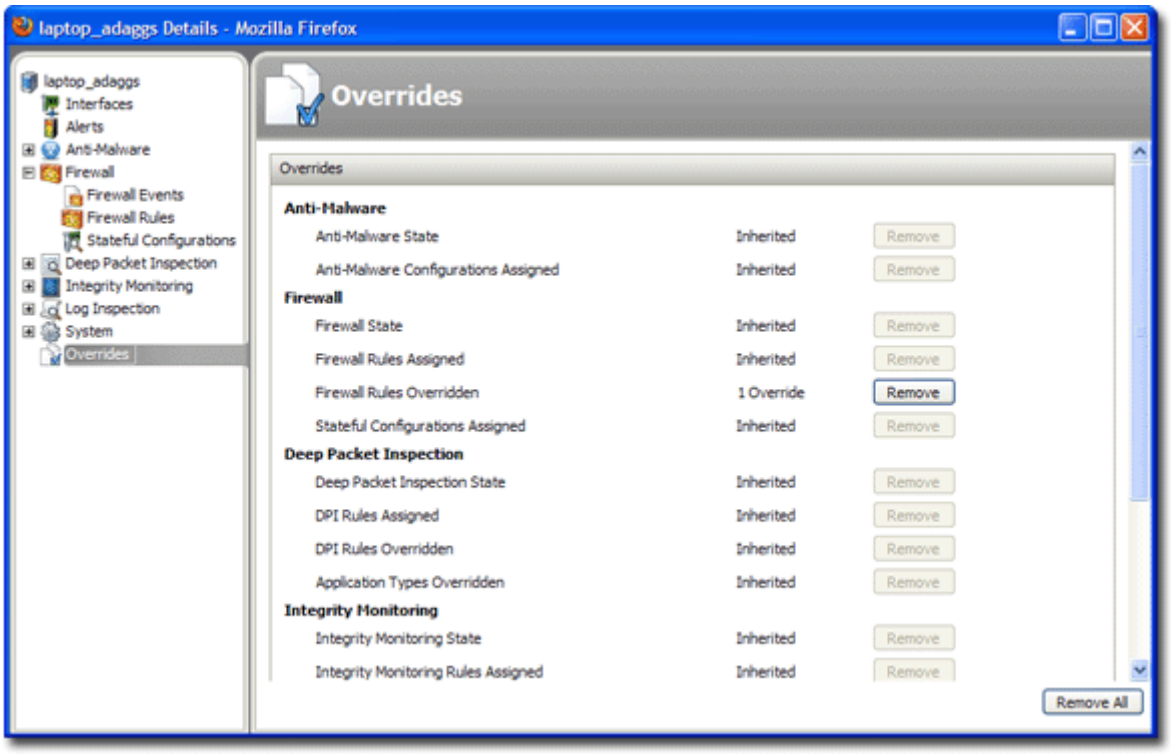


This operation can also be performed at the Security Profile level if the Firewall Rule is part of a Security Profile. You would open the Security Profile's **Details** window and make the same changes. (You could then override those again on a particular computer.)

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Seeing the Overrides on a Computer or Security Profile at a glance

You can see what elements have been overridden on a Security Profile or a computer by opening the Details window and going to the **Overrides** screen.



© Copyright 2011 Trend Micro Inc.
All rights reserved.

Integrity Monitoring Rules Language

The Integrity Monitoring Rules language is a declarative XML-based language that describes the system components and associated attributes that should be monitored by Deep Security. It also provides a means to specify what components within a larger set of components should be excluded from monitoring.

There are two ways to create a new Integrity Monitoring Rule: if you simply want to monitor files for unauthorized changes you can use the "Basic Rule" template. Instructions for using the Basic Rule template can be found in the documentation for the Integrity Monitoring Rules Properties window .

If you want to create a rule that will monitor other Entities on the computer (directories, registry values, services, etc.) you will have to write a rule using the Integrity Monitoring Rules language. (To create a new Integrity Monitoring Rule using the Integrity Monitoring Rules language, go to **Integrity > Integrity Monitoring Rules > New > Content** and select "Custom (XML)".)

Entity Sets

System components included in an Integrity Monitoring Rule are referred to as "Entities". Each type of component is a class of Entity. For example, files, registry keys, and processes are each a class of Entity. The Integrity Monitoring Rules language provides a tag for describing a set of Entities (an Entity Set) for each class of Entity. The following **Entity Set** types are available to be used in a rule:

- **DirectorySet**: rules will scan the integrity of directories
- **FileSet**: rules will scan the integrity of files
- **GroupSet:** rules will scan the integrity of groups
- **InstalledSoftwareSet**: rules will scan the integrity of installed software
- **PortSet:** rules will scan the integrity of listening ports
- **ProcessSet**: rules will scan the integrity of processes
- **RegistryKeySet**: rules will scan registry keys
- **RegistryValueSet**: rules will scan registry values
- **ServiceSet**: rules will scan the integrity of services
- **UserSet:** rules will scan the integrity of users
- **WQLSet:** rules will monitor the integrity of the results of a Windows Management Instrumentation WQL query statement

A single Integrity Rule can contain contain multiple Entity Sets. This allows you to, for example, secure an application with a single rule that monitors multiple files and registry entries.

(This section describes Entity Sets in general. For detailed information about the individual Entity Sets, see their individual pages: DirectorySet, FileSet, GroupSet, InstalledSoftwareSet, PortSet, ProcessSet, RegistryKeySet, RegistryValueSet, ServiceSet, UserSet, and WQLSet.)

Hierarchies and Wildcards

For Entity Sets that represent a hierarchical data type such as FileSet and RegistryKeySet, section-based pattern matching is supported:

- **/ (forward slash)**: demarcates sections of the pattern to be applied to levels of the hierarchy
- **** (two stars)**: matches zero or more sections

The following wildcards are supported:

- **? (question mark)**: matches one character

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- *** (one star)**: matches zero or more characters

"Escaping" characters is also supported:

- **\ (back slash)**: escapes the next character

The pattern is divided into sections using the "/" character, with each section of the pattern being applied to successive levels of the hierarchy as long as it continues to match. For example, if the pattern:

/a?c/123/*.java

is applied to the path:

/abc/123/test.java

Then:

- "a?c" matches "abc"
- "123" matches "abc"
- "*.java" matches "test.java"

When the pattern is applied to the path:

/abc/123456/test.java

Then:

- "a?c" matches "abc"
- "123" does *not* match "123456", and so no more matching is performed

The "**" notation pattern matches zero or more sections, and so:

/abc/**/*.java

matches both "abc/123/test.java" and "abc/123456/test.java". It would also match "abc/test.java" and "abc/123/456/test.java".

Syntax and Concepts

This section will present some example Integrity Monitoring Rules. The examples will use the **FileSet** Entity Set but the topics and components described are common to all Entity Sets. A minimal Integrity Monitoring Rule could look like this:

```
<FileSet base="C:\Program Files\MySQL">
</FileSet>
```

The "base" attribute specifies the base directory for the FileSet. Everything else about the rule will be relative to this directory. If nothing further is added to the rule, everything (including subdirectories) below the "base" will be monitored for changes.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

The "*" and "?" wildcards can be used in a "base" attribute string, but only in the last path component of the base. So this is valid:

```
base="C:\program files\CompanyName * Web Server"
```

but this is not:

```
base="C:\* files\Microsoft Office"
```

Within an Entity Set, "include" and "exclude" tags can be used to control pattern matching. These tags have a "key" attribute that specifies the pattern to match against. The source of the key varies by Entity Set. For example, for Files and Directories it is their path, while for Ports it is the unique protocol/IP/portNumber tuple.

If a path supplied in an include/exclude rule is syntactically invalid, the Agent will generate an "Integrity Monitoring Rule Compile Issue" Agent Event and supply the rule ID and the path (after expansion) as parameters. An example of an invalid path would be `C:\test1\D:\test2` since a file name may not contain two volume identifiers.

Include

The include tag is essentially a white list. Using it means that only those Entities matched by it (or other include tags) will be included. By adding an include tag, the following rule now only monitors changes to files with the name "*.exe" in the "C:\Program Files\MySQL" folder and sub folders:

```
<FileSet base="C:\Program Files\MySQL">
  <include key="**/*.exe"/>
</FileSet>
```

"Includes" can be combined. The following rule will monitor changes to files with the names "*.exe" and "*.dll" in the "C:\Program Files\MySQL" folder and sub folders:

```
<FileSet base="C:\Program Files\MySQL">
  <include key="**/*.exe"/>
  <include key="**/*.dll"/>
</FileSet>
```

It is also possible to combine multiple criteria in a single include block, in which case **all** criteria must be true for a given Entity to be included. The following "include" tag requires that an Entity both end in ".exe" and start with "sample" to be included. Although this requirement could be represented more succinctly, this usefulness of this becomes more apparent as key patterns are combined with other features of the Entity, as described in the "Features" section below.

```
<include>
  <key pattern="**/*.exe"/>
  <key pattern="**/sample*"/>
</include>
```

The following is another way to express the same requirements:

```
<include key="**/*.exe">
  <key pattern="**/sample*"/>
</include>
```

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Exclude

The exclude tag functions as a black list of files, removing files from the set that would otherwise be returned. The following (unlikely) example would place everything but temp files under watch.

```
<FileSet base="C:\Program Files\MySQL">
  <include key="**"/>
  <exclude key="**/*.tmp"/>
</FileSet>
```

The following rule excludes the "MySQLInstanceConfig.exe" from the set of EXEs and DLLs:

```
<FileSet base="C:\Program Files\MySQL">
  <include key="**/*.exe"/>
  <include key="**/*.dll" />
  <exclude key="**/MySQLInstanceConfig.exe"/>
</FileSet>
```

Like the "include" tag, the "exclude" tag can be written to require multiple criteria. The following example shows a multi-criteria "exclude" tag.

```
<exclude>
  <key pattern="**/MySQLInstanceConfig*" />
  <key pattern="**/*.exe" />
</exclude>
```

Case Sensitivity

The case sensitivity of pattern matching for an include/exclude tag may be controlled by the "casesensitive" attribute. The attribute has three allowed values:

- **true**
- **false**
- **platform**

The default value for this attribute is "platform", which means that the case sensitivity of the pattern will match the platform on which it is running. In the following example, both "Sample.txt" and "sample.txt" would be returned on a Windows system, but only "Sample.txt" would be returned on a Unix system:

```
<FileSet base="C:\Program Files\MySQL">
  <include key="**/*Sample*"/>
</FileSet>
```

In this example, only "Sample.txt" would be returned on Windows and Unix:

```
<FileSet base="C:\Program Files\MySQL">
  <include key="**/*Sample*" casesensitive="true"/>
</FileSet>
```

Note that a case sensitive setting of "true" is of limited use on a platform such as Windows which is case insensitive when it comes to most object names.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Features

The inclusion and exclusion of Entities based on features other than their "key" is also supported for some Entity types. The set of features differs by Entity type. The following example will include all executable files. It does not depend on the file extension as previous examples using file extensions did, but instead will check the first few hundred bytes of the file to determine if it is executable on the given OS.

```
<FileSet base="C:\Program Files\MySQL">
  <include key="**" executable="true"/>
</FileSet>
```

Feature attributes must appear in an "include" or "exclude" tag. To use them as part of a multi-criteria include/exclude, they must be specified as attributes of the enclosing include/exclude tag. The following example includes all files that contain the string "MySQL" in their name and are also executable:

```
<include executable="true">
  <key pattern="**/*MySQL*"/>
</include>
```

The previous example can be more succinctly expressed as:

```
<include key="**/*MySQL*" executable="true"/>
```

Some feature attributes are simply matches against the value of one of the Entity's attributes. In such cases, wildcard matches using "*" and "?" are sometimes supported. The help screens for the individual Entity Sets indicate which attributes can be used in include/exclude rules in this way, and whether they support wildcard matching or simple string matching.

Where wildcard matches *are* supported, it is important to note that the match is against the string value of the attribute and that no normalization takes place. Constructs available for Entity key matches such as "**" and the use of "/" to separate hierarchical components don't apply. Matching a path name on Windows requires the use of "\" since that is the character which appears in the value of the attribute being tested, whereas Unix systems will use "/" in path values so matches against Unix paths need to use "/".

The following is an example of a feature match using the "state" attribute:

```
<ServiceSet>
  <include state="running"/>
</ServiceSet>
```

Wildcards are not supported in state matches.

The following example matches any processes where the path of the binary ends in "\notepad.exe":

```
<ProcessSet>
  <include path="*\notepad.exe"/>
</ProcessSet>
```

The following example matches any processes where the command-line begins with "/sbin/":

```
<ProcessSet>
  <include commandLine="/sbin/*"/>
</ProcessSet>
```

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Be careful when using wildcards. A wildcard expression like "**" will look at every file in every sub directory beneath "base". Creating a baseline for such an expression can take a lot of time and resources.

ANDs and ORs

It is possible to express logical ANDs and ORs through the use of multi-criteria includes/excludes and multiple includes/excludes.

There are several ways that a multi criteria include or exclude can be used to express an AND. The most straightforward is to include multiple criteria within a single enclosing tag. The following example shows a simple multi-criteria AND-ing:

```
<include>
  <key pattern="**/*MySQL*" />
  <key pattern="**/*.exe"/>
</include>
```

As well, any criteria expressed as an attribute of the including tag will be grouped with the enclosed criteria as part of the multi-criteria requirement. The following example shows the previous multi-criteria "include" re-written in this way:

```
<include key="**/*.exe">
  <key pattern="**/*MySQL*" />
</include>
```

Finally, if multiple criteria are expressed as attributes of an include/exclude they are treated as an AND:

```
<include executable="true" key="**/*MySQL*" />
```

ORs are expressed simply by the inclusion of multiple include/exclude tags. The following code includes files if their extensions are ".exe" OR ".dll":

```
<include key="**/*.dll" />
<include key="**/*.exe" />
```

Order of Evaluation

All "includes" are processed first, regardless of order of appearance in the rule. If an object name matches at least one "include" tag, it is then tested against the "exclude" tags. It is removed from the set of monitored objects if it matches at least one "exclude" tag.

Entity Attributes

A given Entity has a set of attributes that can be monitored. If no attributes are specified for an Entity Set (i.e. the attributes wrapper tag is not present) then the STANDARD set of attributes for that Entity are assumed. (See the *Shorthand Attributes* sections for the individual Entity Sets.)

However, for a given Entity Set only certain attributes of the Entity may be of interest for Integrity Monitoring. For example, changes to the contents of a log file are most likely expected and allowed. However changes to the permissions or ownership should be reported.

The "attributes" tag of the Entity Sets allows this to be expressed. The "attributes" tag contains a set of tags enumerating the attributes of interest. The set of allowed "attribute" tags varies depending on the Entity Set for which they are being supplied.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

If the "attributes" tag is present, but contains no entries, then the Entities defined by the rule are monitored for existence only.

The following example monitors executable files in "C:\Program Files\MySQL" whose name includes "SQL" for changes to their "last modified", "permissions", and "owner" attributes:

```
<FileSet base="C:\Program Files\MySQL" >
  <include key="**/*SQL*" executable="true"/>
  <attributes>
    <lastModified/>
    <permissions/>
    <owner/>
  </attributes>
</FileSet>
```

The following example monitors the "permissions", and "owner" attributes of log files in "C:\Program Files\MySQL":

```
<FileSet base="C:\Program Files\MySQL" >
  <attributes>
    <permissions/>
    <owner/>
  </attributes>
  <include name="**/*.log" />
</FileSet>
```

In the following example, the STANDARD set of attributes will be monitored. (See Shorthand Attributes, below)

```
<FileSet base="C:\Program Files\MySQL" >
  <include name="**/*.log" />
</FileSet>
```

In the following example, no attributes will be monitored. Only the existence of the Entities will be tracked for change.

```
<FileSet base="C:\Program Files\MySQL" >
<attributes/>
<include name="**/*.log" />
</FileSet>
```

Shorthand Attributes

Shorthand attributes provide a way to specify a group of attributes using a single higher level attribute. Like regular attributes the set of allowed values differs based on the Entity Set for which they are being supplied.

Shorthand Attributes are useful in cases where a set of attributes naturally group together, in cases where exhaustively listing the set of attributes would be tedious, and in cases where the set of attributes represented by the high level attribute may change with time or system configuration. Examples of each case follows:

Attribute	Description
STANDARD	The set of attributes to monitor for the Entity Set. This is different than "every possible attribute" for the Entity Set. For example, it would not include every possible hash algorithm, just the ones deemed sufficient. For the list of "standard" attributes for each Entity Set, see

© Copyright 2011 Trend Micro Inc.
All rights reserved.

	sections for the individual Entity Sets.
CONTENTS	This is Shorthand for the hash, or set of hashes, of the contents of the file. Defaults to SHA-1.

onChange

An EntitySet may be set to monitor changes in real time. If the onChange attribute of an EntitySet is set to true (the default value) then the entities returned by the EntitySet will be monitored for changes in real time. When a change is detected the Entity is immediately compared against its baseline for variation. If an Entity set is not onChange, it will be run only when a baseline is built or when it is triggered via a Scheduled Task or on demand by the Deep Security Manager.

The following sample monitors the MySQL binaries in real time:

```
<FileSet base="C:\Program Files\MySQL" onChange="true">
<include key="**/*.exe"/>
<include key="**/*.dll" />
</FileSet>
```

Environment Variables

Environment variables can be included in the base value used in Entity Sets. They are enclosed in "${}". The variable name itself is prefaced with "env.".

The following example sets the base directory of the FileSet to the path stored in the PROGRAMFILES environment variable:

```
<FileSet base="${env.PROGRAMFILES}"/>
```

The values of referenced environment variables are read and stored by the Deep Security Agent on Agent startup. If the value of an environment variable changes, the Agent must be restarted to register the change.

If a referenced environment variable is not found, the Entity Sets referencing it are not scanned or monitored, but the rest of the configuration is used. An alert is triggered indicating that the variable is not present. The Agent reports an invalid environment variable using Agent Event "Integrity Monitoring Rule Compile Issue". The ID of the Integrity Monitoring Rule and the environment variable name are supplied as parameters to the Event.

Deep Security Agents versions prior to 6.0.0.2027 do not detect environment variable value changes. They expand the values when a new configuration is received, but do not check at startup time for changes. Version 6.0.0.2027 checks for changes at startup and every time new Integrity Monitoring Rules are received. If an Integrity Monitoring Rule contains an environment variable reference that was originally valid but at some point becomes invalid, the Deep Security Agent treats the Integrity Monitoring Rule as though a new version of it was received from the Manager. A new baseline for the entire Integrity Monitoring Rule is calculated, with the Entity Set(s) that have invalid references omitted.

Registry values

Registry values can be included in the base value used in Entity Sets. They are enclosed in ${}. The path to the registry value itself is prefaced with "reg.". The following example sets the base directory of the FileSet to the path stored in the *"HKLM\Software\Trend Micro\Deep Security Agent\InstallationFolder*" registry value:

© Copyright 2011 Trend Micro Inc.
All rights reserved.

<FileSet base="${reg.HKLM\Software\Trend Micro\Deep Security Agent\InstallationFolder}"/>

The values of referenced registry values are read when a new or changed rule is sent to the Agent. The Agent also checks all rules at startup time and will rebuild the baseline for affected rules if any referenced registry values change.

If a referenced registry value is not found, the Entity Sets referencing it are not scanned or monitored, but the rest of the configuration is used. An alert notifying you that the variable is not present is triggered. The Agent reports an invalid environment variable expansion using Agent Event "Integrity Monitoring Rule Compile Issue". The ID of the Integrity Monitoring Rule and the registry value path are supplied as parameters to the event.

The following example monitors key MS Office files for changes. Note the use of environment variables and wildcards:

```
<FileSet base="${env.ProgramFiles}\Common Files\MS Shared\Office*">
  <include "**/*" executable="true"/>
  <include "**/*.dot"/>
</FileSet>
<FileSet base="${env.ProgramFiles}\MS Office">
  <include "**/*" executable="true"/>
  <include "**/*.dot"/>
</FileSet>
<RegistryValueSet base="HKLM\Software\MS\Office">
  <include "**/*"/>
</RegistryValueSet>
<RegistryValueSet base="HKEY_USERS\*\Software\MS\Office">
  <include "**/*"/>
</RegistryValueSet>
```

Use of ".."

The ".." convention for referencing a parent directory is supported starting in Deep Security Agent version 6.0.0.2060. The Agent will attempt to normalize base directory names for FileSet and DirectorySet elements by resolving ".." references and converting Windows short names to long names. For example, on Vista the following FileSet would have a base directory of "C:\Users". On pre-Vista versions of Windows it would be "C:\Documents and Settings"

```
<FileSet base="${env.USERPROFILE}\..">
  <include key="*/Start Menu/Programs/Startup/*"/>
</FileSet>
```

Best Practices

Rules should be written to only include objects and attributes that are of significance. This will ensure that no events are reported if other attributes of the object change. For example, your change monitoring policy may place restrictions on permission and ownership of files in "`/bin`". Your Integrity Monitoring Rule should monitor owner, group, and permissions, but not other attributes like lastModified or hash values.

When using Integrity Monitoring Rules to detect malware and suspicious activity, monitor services, watch for use of NTFS data streams, and watch for executable files in unusual places such as "`/tmp`" or "`${env.windir}\temp`".

Always be as specific as possible when specifying what objects to include in a rule. The fewer objects you include, the less time it will take to create your baseline and the less time it will take to scan for changes. Exclude objects which are expected to change and only monitor the attributes you are concerned about.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Do not:

- Use "`**/...` " from a top-level of the hierarchy such as "`/`", "`C:\`", or "`HKLM\Software`"
- Use more than one content hash type unless absolutely necessary
- Reference user-specific locations such as `HKEY_CURRENT_USER`, `${env.USERPROFILE}`, or `${env.HOME}`

Any of these statements in your Integrity Monitoring Rules will cause performance issues as the Deep Security Agent searches through many items in order to match the specified patterns.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

DirectorySet

The DirectorySet tag describes a set of Directories.

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
base	Sets the base directory of the DirectorySet. Everything else in the tag is relative to this directory	Yes	N/A	String values resolving to syntactically valid path (Path is not required to exist) **Note**: UNC paths are allowed by Windows Agents, but require that the remote system allow access by the "LocalSystem" account of the Agent computer. The Agent is a Windows service and runs as LocalSystem, aka NT AUTHORITY\SYSTEM. When accessing a network resource, the LocalSystem uses the computer's credentials, which is an account named *DOMAIN\MACHINE*$. The access token presented to the remote computer also contains the "Administrators" group for the computer, so remote shares must grant read privileges to either the Agent computer's account, the Agent computer's Administrators group, or "Everyone". For testing access to UNC paths, use this technique to launch a Windows command prompt running as a service under the LocalSystem account. With that you can try accessing network & local resources, or launch other applications that will run under the LocalSystem account. If the base value is not syntactically valid, the FileSet will not be processed. The rest of the config will be evaluated.
onChange	Whether the directories returned should be monitored in real time.	No	false	true, false
followLinks	Will this DirectorySet follow symbolic links.	No	false	true, false

Entity Set Attributes

These are the attributes of the Entity that may be monitored by Integrity Monitoring Rules.

- **Created:** Timestamp when the file was created
- **LastModified:** Timestamp when the file was last modified
- **LastAccessed:** Timestamp when the directory was last accessed. On Windows this value does not get updated immediately, and recording of the last accessed timestamp can be disabled as a performance enhancement. See File Times for details. The other problem with this attribute is that the act of scanning a directory requires that the Agent open the directory, which will change its last accessed timestamp.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **Permissions:** The directory's security descriptor (in SDDL format) on Windows or Posix-style ACLs on Unix systems that support ACLs, otherwise the Unix style rwxrwxrwx file permissions in numeric (octal) format.
- **Owner:** User ID of the directory owner (commonly referred to as the "UID" on Unix)
- **Group:** Group ID of the directory owner (commonly referred to as the "GID" on Unix)
- **Flags:** Windows-only. Flags returned by the GetFileAttributes() Win32 API. Windows Explorer calls these the "Attributes" of the file: Readonly, Archived, Compressed, etc.
- **SymLinkPath:** If the directory is a symbolic link, the path of the link is stored here. On Windows, use the SysInternals "junction" utility to create the Windows equivalent of symlinks.
- **InodeNumber (Unix-only):**
- **DeviceNumber (Unix-only):** Device number of the disk on which the inode associated with the directory is stored

Short Hand Attributes

The following are the Short Hand Attributes, and the attributes to which they map.

- **STANDARD:** Created LastModified Permissions Owner Group Flags (Windows only) SymLinkPath

Meaning of "Key"

Key is a pattern to match against the path of the directory relative to the directory specified by "dir". This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the path separated by the file separator of the given OS.

Sub Elements

- **Include**
- **Exclude**

See the general description of include/exclude for their allowed attributes and sub elements. Only information specific to include/excludes relating to this EntitySet class are included here.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

FileSet

The FileSet tag describes a set of Files.

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
base	Sets the base directory of the FileSet. Everything else in the tag is relative to this directory.	Yes	N/A	String values resolving to syntactically valid path (Path is not required to exist). **Note**: UNC paths are allowed by Windows Agents, but require that the remote system allow access by the "LocalSystem" account of the Agent computer. The Agent is a Windows service and runs as LocalSystem, aka NT AUTHORITY\SYSTEM. When accessing a network resource, the LocalSystem uses the computer's credentials, which is an account named *DOMAIN**MACHINE*$. The access token presented to the remote computer also contains the "Administrators" group for the computer, so remote shares must grant read privileges to either the Agent computer's account, the Agent computer's Administrators group, or "Everyone". For testing access to UNC paths, use this technique to launch a Windows command prompt running as a service under the LocalSystem account. With that you can try accessing network & local resources, or launch other applications that will run under the LocalSystem account. If the base value is not syntactically valid, the FileSet will not be processed. The rest of the config will be evaluated.
onChange	Whether the files returned should be monitored in real time.	No	false	true, false
followLinks	Will this FileSet follow symbolic links. (added in Agent version 6.0.0.637)	No	false	true, false

Entity Set Attributes

These are the attributes of the FileSet that can be monitored by Integrity Monitoring Rules.

- **Created:** Timestamp when the file was created
- **LastModified:** Timestamp when the file was last modified
- **LastAccessed:** Timestamp when the file was last accessed. On Windows this value does not get updated immediately, and recording of the last accessed timestamp can be disabled as a performance enhancement. See File Times for details. The other problem with this attribute is that the act of scanning a file requires that the Agent open the file, which will change its last accessed

© Copyright 2011 Trend Micro Inc.
All rights reserved.

timestamp. On Unix, the Agent will use the O_NOATIME flag if it is available when opening the file, which prevents the OS from updating the last accessed timestamp and speeds up scanning.

- **Permissions:** The file's security descriptor (in SDDL format) on Windows or Posix-style ACLs on Unix systems that support ACLs, otherwise the Unix style rwxrwxrwx file permissions in numeric (octal) format.
- **Owner:** User ID of the file owner (commonly referred to as the "UID" on Unix)
- **Group:** Group ID of the file owner (commonly referred to as the "GID" on Unix)
- **Size:** size of the file
- **Sha1:** SHA-1 hash
- **Sha256:**SHA-256 hash
- **Md5:** MD5 hash
- **Flags:** Windows-only. Flags returned by the GetFileAttributes() Win32 API. Windows Explorer calls these the "Attributes" of the file: Readonly, Archived, Compressed, etc.
- **SymLinkPath** (Unix only): If the file is a symbolic link, the path of the link is stored here. Windows NTFS supports Unix-like symlinks, but only for directories, not files. Windows shortcut objects are not true symlinks since they are not handled by the OS; the Windows Explorer handles shortcut files (*.lnk) but other applications that open a *.lnk file will simply see the contents of the lnk file.
- **InodeNumber** (Unix only)
- **DeviceNumber** (Unix only): Device number of the disk on which the inode associated with the file is stored
- **BlocksAllocated** (Unix only)
- **Growing:** (DSA 7.5+) contains the value "true" if the size of the file stays the same or increases between scans, otherwise "false". This is mainly useful for log files that have data appended to them. Note that rolling over a log file will trigger a change in this attribute.
- **Shrinking:** (DSA 7.5+) contains the value "true" if the size of the file stays the same or decreases between scans, otherwise "false".

Short Hand Attributes

The following are the Short Hand Attributes, and the attributes to which they map.

- **CONTENTS:** Resolves to the content hash algorithm set in the DSM in **System > System Settings > Integrity Monitoring**.
- **STANDARD:** Created, LastModified, Permissions, Owner, Group, Size, Contents, Flags (Windows only), SymLinkPath (Unix only)

Drives Mounted as Directories

Drives mounted as directories are treated as any other directory, unless they are a network drive in which case they are ignored.

Alternate Data Streams

NTFS based filesystems support the concept of alternate data streams. When this feature is used it behaves conceptually like files within the file.

To demonstrate this, type the following at the command prompt:

```
echo plain > sample.txt
echo alternate > sample.txt:s
more < sample.txt
more < sample.txt:s
```

The first "more" will show only the text "plain", the same text that will be displayed if the file is opened with a standard text editor, such as notepad. The second "more", which accesses the "s" stream of sample.txt will display the string "alternate".

© Copyright 2011 Trend Micro Inc.
All rights reserved.

For FileSets, if no stream is specified, then all streams are included. Each stream is a separate Entity entry in the baseline. The available attributes for streams are:

- **size**
- **Sha1**
- **Sha256**
- **Md5**
- **Contents**

The following example would include both streams from the demonstration above:

```
<include key="**/sample.txt" />
```

To include or exclude specific streams, the ":" notation is used. The following example matches only the "s" stream on sample.txt and not the main sample.txt stream:

```
<include key="**/sample.txt:s" />
```

Pattern matching is supported for the stream notation. The following example would include sample.txt, but exclude all of its alternate streams:

```
<include key="**/sample.txt" />
<exclude key="**/sample.txt:*" />
```

Meaning of "Key"

Key is a pattern to match against the path of the file relative to the directory specified by "base". This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the path separated by the file separator of the given OS

Sub Elements

- **Include**
- **Exclude**

See the general description of include/exclude for their allowed attributes and sub elements. Only information specific to include/excludes relating to the FileSet Entity Set class are included here.

Special attributes of Include/Exclude for FileSets:

executable

Determines if the file is executable. This does not mean that its permissions allow it to be executed. Instead the contents of the file are checked, as appropriate for platform, to determine if the file is an executable file.

Note that this is a relatively expensive operation since it requires the Agent to open the file and examine the first kilobyte or two of its content looking for a valid executable image header. Opening and reading every file is much more expensive than simply scanning directories and matching filenames based on wildcard patterns, so any include/exclude rules using "executable" will result in slower scan times than those that do not use it.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

GroupSet

Support for GroupSet elements is available as of DSA 7.0.0.596

GroupSet represents a set of groups. Note these are local groups only.

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
onChange	Will be monitored in real time	No	false	true, false

Entity Set Attributes

These are the attributes of the entity that can be monitored:

- **Description:** (Windows only) The textual description of the group.
- **Group:** The group ID and name. The group name is part of the entity key, but it's still important to be able to monitor the group ID/name pairing in case groups are renamed and given new IDs. Operating systems generally enforce security based on its ID.
- **Members:** A comma separated list of the members of the group.
- **SubGroups:** (Windows only) A comma separated list of sub-groups of the group.

Short Hand Attributes

- **Standard:** Group Members SubGroups

Meaning of "Key"

The key is the group's name. This is not a hierarchical EntitySet. Patterns are applied only to the group name. As a result the "**" pattern is not applicable. The following example monitors the "Administrators" group for additions/deletions. (The "Member" attribute is included implicitly because it is a part of the STANDARD set, and no attributes are explicitly listed.)

```
<GroupSet>
  <include key="Administrators" />
</GroupSet>
```

Sub Elements

Include Exclude

See the general description of include/exclude for their allowed attributes and sub elements.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

InstalledSoftwareSet

Represents a set of installed software. The make-up of the "key" used to uniquely identify an installed application is platform-specific, but it is often a shorthand version of the application name or a unique numeric value.

On Windows the key can be something readable like "FogBugz Screenshot_is1" or it can be a GUID like "{90110409-6000-11D3-8CFE-0150048383C9}". You can examine these by looking at the subkeys of HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

On Linux the key is the RPM package name, as shown by the command:

rpm -qa --qf "%{NAME}\n"

On Solaris the key is the package name as shown by the **pkginfo** command.

On HPUX the key is the application name as shown by the command:

/usr/sbin/swlist -a name

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
onChange	Will be monitored in real time	No	false	true, false

Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules. Presence of the attributes is dependent on both the platform and the application itself - installation programs do not necessarily populate all of the attributes.

- **Manufacturer:** The publisher or manufacturer of the application
- **Name:** The friendly name or display name of the application. (Not available on Linux.)
- **InstalledDate:** Date of installation. (Not available on AIX) This is normally returned as YYYY-MM-DD [HH:MM:SS], but many installers on Windows format the date string in a different manner so this format is not guaranteed.
- **InstallLocation:** The directory where the application is installed. (Only available on Windows, Solaris, and HPUX)
- **Parent:** For patches and updates, this gives the key name of this item's parent. Only available on Windows.
- **Size:** The estimated size of the application, if available. On Solaris this attribute is monitored as of DSA 7.0.0.647. On Windows this attribute is monitored as of DSA 7.0.0.802, and comes from the "EstimatedSize" registry value under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*. The value in that location is expressed in KB, so the DSA multiplies it by 1024 before returning it. Note that not all Windows applications populate the EstimatedSize field in the registry. (This attribute is not available on AIX.)
- **Version:** The version of the installed application. On Windows this comes from the "DisplayVersion" registry value.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Short Hand Attributes

These are the short hand attributes of the Entity and the attributes to which they resolve

- **STANDARD:** InstalledDate, Name, Version

Meaning of "Key"

The key is the name of the installed software. This is not a hierarchical key, so the ** pattern does not apply. On Windows the key is often a GUID, especially for anything installed via the Windows Installer (aka MSI). Use the name="XXX" feature if you need to include/exclude based on the display name rather than the GUID.

The following example would monitor for the addition and deletion of new software.

```
<InstalledSoftwareSet>
  <include key="*"/>
  <attributes/>
</InstalledSoftwareSet>
```

Sub Elements

- **Include**
- **Exclude**

See the general description of include/exclude for their allowed attributes and sub elements. Only information specific to include/excludes relating to this EntitySet class are included here.

Special attributes of Include/Exclude for InstalledSoftwareSets:

name (Windows only)

Allows wildcard matching using ? and * on the display name of the application (the "name" attribute of the Entity). For example:

```
<InstalledSoftwareSet>
  <include name="Microsoft*"/>
<InstalledSoftwareSet>
```

will match all installed applications whose display name (as shown by the Control Panel) starts with "Microsoft".

manufacturer

Allows wildcard matching using ? and * on the publisher or manufacturer of the application. For example:

```
<InstalledSoftwareSet>
  <include manufacturer="* Company "/>
<InstalledSoftwareSet>
```

will match all installed applications whose manufacturer ends with " Company ".

© Copyright 2011 Trend Micro Inc.
All rights reserved.

PortSet

Represents a set of listening ports.

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
onChange	Will be monitored in real time	No	false	true, false

Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **Created:** Windows only - XP SP2+ and Server 2003 SP1+ required. Returned by the GetExtendedTcpTable() or GetExtendedUdpTable() API. Indicates when the bind operation that created this TCP/UDP link occurred.
- **Path:** Windows only - XP SP2+ and Server 2003 SP1+ required. Gives the short name, if available, of the module that owns the port. On Windows this comes from the GetOwnerModuleFromXxxEntry() APIs. According to Microsoft documentation, the resolution of connection table entries to owner modules is a best practice. In a few cases, the owner module name returned can be a process name, such as "svchost.exe", a service name (such as "RPC"), or a component name, such as "timer.dll".
- **Process:** (Windows only - XP SP2+ and Server 2003 SP1+ required.) Gives the full path, if available, of the module that owns the port. On Windows this comes from the GetOwnerModuleFromXxxEntry() APIs. According to Microsoft documentation, the resolution of connection table entries to owner modules is a best practice.
- **ProcessId:** (Windows only - XP SP2+ and Server 2003 SP1+ required.) Gives the PID of the process that issued the bind for this port.
- **User:** (Linux only). Gives the user that owns the port.

Meaning of "Key"

The key is in the following format:

<PROTOCOL>/<IP ADDRESS>/<PORT>

For example:

tcp/172.14.207.94/80
udp/172.14.207.94/68

IPV6

If the IP address is IPv6 the key is in the same format, but the protocol is TCP6 or UDP6 and the IP address is an IPv6 address as returned by the getnameinfo API:

tcp6/3ffe:1900:4545:3:200:f8ff:fe21:67cf/80
udp6/3ffe:1900:4545:3:200:f8ff:fe21:67cf/68

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Matching of the Key

This is not a hierarchical key, so ** is not applicable. Unix-style glob matching is possible using * and ?. The following pattern matches port 80 on the IP addresses 72.14.207.90 through 72.14.207.99:

*/72.14.207.9?/80

The following pattern matches port 80 on the IP addresses 72.14.207.2, 72.14.207.20 through 72.14.207.29 as well as 72.14.207.200 through 72.14.207.255:

/72.14.207.2/80

The following pattern matches port 80 on any IP.

*/80

The following example would monitor for any change in the listening ports but ignore port 80 for TCP in IPV4 and IPV6:

```
<PortSet>
  <include key="*"/>
  <exclude key="tcp*/*/80"/>
</PortSet>
```

Sub Elements

- **Include**
- **Exclude**

See the general description of include/exclude for their allowed attributes and sub elements. Only information specific to include/excludes relating to this EntitySet class are included here.

Special attributes of Include/Exclude for PortSets:

Various other attributes of the port may be used in include/exclude *feature* tests. These tests compare a value against the value of an attribute of the port; take note of the platform support for various attributes - not all attributes are available across platforms or even platform revisions, hence the use of these tests in include/exclude tags is of limited use. The feature tests support Unix glob-style wildcarding with * and ?, and there is no normalization of path separators or other characters - it is a simple match against the value of the attribute.

Path

Checks for a wildcard match against the path attribute of the port. The following example would monitor ports owned by processes running the main IIS binary:

```
<PortSet>
  <include path="*\system32\inetsrv\inetinfo.exe"/>
</PortSet>
```

Process

Checks for a wildcard match against the process attribute of the port. The following example would monitor ports owned by anything running in a svchost.exe or outlook.* binary:

© Copyright 2011 Trend Micro Inc.
All rights reserved.

```
<PortSet>
  <include process="svchost.exe"/>
  <include process="outlook.*"/>
</PortSet>
```

User

Checks for a wildcard match against the user attribute of the port. The following example would monitor ports on a Unix system that were owned by the super-user (root):

```
<PortSet>
  <include user="root"/>
</PortSet>
```

© Copyright 2011 Trend Micro Inc.
All rights reserved.

ProcessSet

Represents a set of processes.

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
onChange	Will be monitored in real time	No	false	true, false

Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **CommandLine:** The full command-line as shown by "ps -f" (Unix), "ps w" (Linux), or Process Explorer (Windows).
- **Group:** The group under which the process is running. Under Unix this is the "effective" group ID of the process, which can change over time if the process drops privileges or otherwise switches its effective group credentials. On Windows this is the current Primary Group of the process as returned by the Win32 API GetTokenInformation with a TokenInformationClass of TokenPrimaryGroup. This is the default Primary Group SID for newly created objects. In addition to a Primary Group, processes typically have one or more group credentials associated with them. Those additional group credentials are not monitored by the Agent - they can be viewed on the "Security" tab of the process properties in Process Explorer.
- **Parent:** The PID of the process that created this process.
- **Path:** The full path to the binary of the process. Not available on Solaris 8 & 9 nor HP-UX. On Windows this comes from the GetModuleFileNameEx() API. On Linux and Solaris 10 it comes from reading the symlink /proc/{pid}/exe or /proc/{pid}/path/a.out respectively.
- **Process:** The short name of the process binary (no path). For example, for "c:\windows\notepad.exe" it would be "notepad.exe" and for "/usr/local/bin/httpd" it would be "httpd".
- **Threads:** The number of threads currently executing in the process. Not available on HP-UX.
- **User:** The user under which the process is running. Under Unix this is the "effective" user ID of the process, which can change over time if the process drops privileges or otherwise switches its effective user credentials.

Short Hand Attributes

- **STANDARD:** CommandLine, Group, Parent, Path (where available), Process User

Meaning of "Key"

The key is a combination of the "Process" attribute (the short name of the executable) and the PID. The PID is appended to the name with a path separator in between, ex. notepad.exe\1234 on Windows and httpd/1234 on Unix. The use of the path separator is to allow include/exclude matching of key="abc/*" to work as expected.

Sub Elements

- **Include**

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **Exclude**

See the general description of include for their allowed attributes and sub elements. Only information specific to include/excludes relating to this EntitySet class are included here.

Special attributes of Include/Exclude for ProcessSets:

The following example would monitor the set of running processes for notepad.exe regardless of the PID.:

```
<ProcessSet>
  <include key="notepad.exe/*" />
</ProcessSet>
```

Various other attributes of a process can be used in include/exclude *feature* tests. The feature tests support Unix glob-style wildcarding with * and ?, and there is no normalization of path separators or other characters - it is a simple glob-style match against the value of the attribute.

CommandLine

Checks for a wildcard match against the commandLine attribute of the process. The following example would monitor any process whose command-line matches "*httpd *":

```
<ProcessSet>
  <include commandLine="*httpd *" />
</ProcessSet>
```

Group

Checks for a wildcard match against the group attribute of the process. The text version of the group name is used rather than the numeric form: use "daemon" rather than "2" to test for the daemon group on Linux. The following example would monitor any process running as one of the groups root, daemon, or lp:

```
<ProcessSet>
  <include group="root" />
  <include group="daemon" />
  <include group="lp" />
</ProcessSet>
```

Path

Checks for a wildcard match against the path attribute of the process. The path attribute is not available on some platforms. The following example would monitor any process whose binary resides under System32:

```
<ProcessSet>
  <include path="*\System32\*" />
</ProcessSet>
```

User

Checks for a wildcard match against the user attribute of the process. The text version of the user name is used rather than the numeric form: use "root" rather than "0" (zero) to test for the superuser on Unix. The following example would monitor any process running as one of the built in system users (ex. NT AUTHORITY\SYSTEM, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE):

© Copyright 2011 Trend Micro Inc.
All rights reserved.

```
<ProcessSet>
  <include user="NT AUTHORITY\*" />
</ProcessSet>
```

© Copyright 2011 Trend Micro Inc.
All rights reserved.

RegistryKeySet

The RegistryKeySet tag describes a set keys in the registry (Windows only).

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
base	Sets the base key of the RegistryKeySet. Everything else in the tag is relative to this key. The base must begin with one of the following registry branch names: HKEY_CLASSES_ROOT (or HKCR), HKEY_LOCAL_MACHINE (or HKLM), HKEY_USERS (or HKU), HKEY_CURRENT_CONFIG (or HKCC)	Yes	N/A	String values resolving to syntactically valid registry key path

Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **Owner**
- **Group**
- **Permissions**
- **LastModified** ("LastWriteTime" in Windows registry terminology)
- **Class**
- **SecurityDescriptorSize**

Short Hand Attributes

- **STANDARD:** Group, Owner, Permissions, LastModified

Meaning of "Key"

Registry Keys are stored hierarchically in the registry, much like directories in a file system. For the purpose of this language the "key path" to a key is considered to look like the path to a directory. For example the "key path" to the "Deep Security Agent" key of the Agent would be:

HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\Deep Security Agent

The "key" value for includes/excludes for the RegistryValueSet is matched against the key path. This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the key path separated by "\".

Sub Elements

- **Include**
- **Exclude**

© Copyright 2011 Trend Micro Inc.
All rights reserved.

See the general description of include for their allowed attributes and sub elements.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

RegistryValueSet

A set of Registry values (Windows only).

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
base	Sets the base key of the RegistryValueSet. Everything else in the tag is relative to this key. The base must begin with one of the registry branch names: HKEY_CLASSES_ROOT (or HKCR), HKEY_LOCAL_MACHINE (or HKLM), HKEY_USERS (or HKU), HKEY_CURRENT_CONFIG (or HKCC)	Yes	N/A	String values resolving to syntactically valid registry key

Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules:

- Size
- Type
- Sha1
- Sha256
- Md5

Short Hand Attributes

- **CONTENTS:** Resolves to the content hash algorithm set in the DSM in **System > System Settings > Integrity Monitoring**.
- **STANDARD:** Size, Type, Contents

Meaning of "Key"

Registry Values are name/value pairs stored under a key in the registry. The key under which they are stored may in turn be stored under another key, very much like files and directories on a file system. For the purpose of this language the "key path" to a value is considered to look like the path to a file. For example, the "key path" to the InstallationFolder value of the Agent would be:

HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\Deep Security Agent\InstallationFolder

The "key" value for includes/excludes for the RegistryValueSet is matched against the key path. This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the key path separated by "\"

Default Value

Each registry key has an unnamed or default value.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

This is present for legacy support: http://blogs.msdn.com/oldnewthing/archive/2008/01/18/7145021.aspx

This value can be explicitly specified for inclusion/exclusion by using a trailing "/" in patterns. For example, "**/" will match all subordinate unnamed values, and "*Agent/**/" will match all unnamed values below a key matching "*Agent".

Note that registry value names may contain any printable character, including quotes, backslash, the "@" symbol, etc.

The Agent deals with this in Entity key names by using backslash as an escape character, but only backslashes themselves are escaped. It does this so that it can tell the difference between a value name containing a backslash and a backslash that occurs as part of the registry path. This means that value names which end with a backslash character will match rules designed to match the default/unnamed value.

See the table below for example registry value names and the resulting Entity key.

Value	Escaped Form	Example
Hello	Hello	HKLM\Software\Sample\Hello
"Quotes"	"Quotes"	HKLM\Software\Sample\"Quotes"
back\slash	back\\slash	HKLM\Software\Sample\back\\slash
trailing\	trailing\\	HKLM\Software\Sample\trailing\\
		HKLM\Software\Sample\
@	@	HKLM\Software\Sample\@

Sub Elements

- **Include**
- **Exclude**

See the general description of include/exclude for their allowed attributes and sub elements.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

ServiceSet

The ServiceSet element represents a set of services (Windows only). Services are identified by the "service name", which is not the same as the "name" column shown in the Services administrative tool. The service name can be seen in the service properties and is often shorter than the value shown in the "name" column, which is actually the "Display Name" of the service. For example, the Agent has a service name of "ds_agent" and a display name of "Trend Micro Deep Security Agent".

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
onChange	Will be monitored in real time	No	false	true, false

Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **Permissions:** The service's security descriptor in SDDL format.
- **Owner:** User ID of the service owner
- **Group:** Group ID of the service owner
- **BinaryPathName:** The path plus optional command-line arguments that Windows uses to start the service.
- **DisplayName:** The "display name" of the service as shown in the properties panel of the service.
- **Description:** Description as it appears in the Services panel
- **State:** The current state of the service. One of: stopped, starting, stopping, running, continuePending, pausePending, paused
- **StartType:** How is the service started? One of: automatic, disabled, manual.
- **LogOnAs:** The name of the account that the service process will be logged on as when it runs.
- **FirstFailure:** Action to take the first time the service fails. Format is "delayInMsec,action", where action is one of None, Restart, Reboot, RunCommand.
- **SecondFailure:** Action to take the first time the service fails. Format is "delayInMsec,action", where action is one of None, Restart, Reboot, RunCommand.
- **SubsequentFailures:** Action to take the first time the service fails. Format is "delayInMsec,action", where action is one of None, Restart, Reboot, RunCommand.
- **ResetFailCountAfter:** Time after which to reset the failure count to zero if there are no failures, in seconds.
- **RebootMessage:** Message to broadcast to server users before rebooting in response to the "Reboot" service controller action.
- **RunProgram:** Full command line of the process to execute in response to the RunCommand service controller action.
- **DependsOn:** Comma separated list of components that the service depends on
- **LoadOrderGroup:** The load ordering group to which this service belongs. The system startup program uses load ordering groups to load groups of services in a specified order with respect to the other groups. The list of load ordering groups is contained in the following registry value: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ServiceGroupOrder
- **ProcessId:** This is the numeric ID of the process that hosts the service. Many services may exist in a single Windows process, but for those that run in their own process, the monitoring of this attribute will allow the system to log service restarts.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Short Hand Attributes

These are the short hand attributes of the Entity and the attributes to which they resolve

- **STANDARD**: Permissions, Owner, Group, BinaryPathName, Description, State, StartType, LogOnAs, FirstFailure, SecondFailure, SubsequentFailures, ResetFailCountAfter, RunProgram, DependsOn, LoadOrderGroup, ProcessId

Meaning of "Key"

The key is the Service's name, which is not necessarily the same as the "name" column shown in the Services administrative tool (that tool shows the "display name" of the service). The service name can be seen in the service properties and is often shorter than the value shown in the "name" column.

This is not a hierarchical Entity Set. Patterns are applied only to the service name. As a result the ** pattern is not applicable.

Sub Elements

- **Include**
- **Exclude**

See the general description of include for their allowed attributes and sub elements. Only information specific to include/excludes relating to this Entity Set class are included here.

Special attributes of Include/Exclude for ServiceSets:

state

Include/exclude based on whether the state of the service (stopped, starting, stopping, running, continuePending, pausePending, paused). The following example would monitor the set of running services for change:

```
<ServiceSet>
  <include state="running"/>
</ServiceSet>
```

© Copyright 2011 Trend Micro Inc.
All rights reserved.

UserSet

Support for UserSet elements is available as of DSA 7.0.0.507

The UserSet element represents a set of users. On a Windows system it operates on users local to the system - the same users displayed by the "Local Users and Groups" MMC snap-in. Note that these are *local* users only if the DSA is running on something other than a domain controller. On a domain controller a UserSet element will enumerate all of the domain users, which may not be advisable for extremely large domains.

On Unix systems, the users monitored are whatever the "getpwent_r()" and "getspnam_r()" APIs have been configured to return.

Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

Attribute	Description	Required	Default Value	Allowed Values
onChange	Will be monitored in real time	No	false	true, false

Entity Set Attributes

These are the attributes of the entity that can be monitored:

Common Attributes

- **cannotChangePassword:** True/false indicating if the user is permitted to change their password.
- **disabled:** True/false indicating if the account has been disabled. On Windows systems this reflects the "disabled" checkbox for the user. On Unix systems this will be true if the user's account has expired or if their password has expired and they've exceeded the inactivity grace period for changing it.
- **fullName:** The display name of the user.
- **groups:** A comma-separated list of the groups to which the user belongs.
- **homeFolder:** The path to the home folder or directory.
- **lockedOut:** True/false indicating if the user has been locked out, either explicitly or due to excessive failed password attempts.
- **passwordHasExpired:** True/false indicating if the user's password has expired. Note that on Windows this attribute is only available on Windows XP and newer operating systems. (N/A in AIX)
- **passwordLastChanged:** The timestamp of the last time the user's password was changed. This is recorded by the DSA as the number of milliseconds since Jan 1 1970 UTC - DSM renders the timestamp in local time based on this value. Note that on Unix platforms the resolution of this attribute is one day, so the time component of the rendered timestamp is meaningless. (N/A in AIX)
- **passwordNeverExpires:** True/false indicating if the password does not expire.
- **user:** The name of the user as known to the operating system. For example, "Administrator" or "root".

Windows-only Attributes

- **description:** The primary group the user belongs to.
- **homeDriveLetter:** The drive letter to which a network share is mapped as the user's home folder.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

- **logonScript:** The path to a script that executes every time the user logs in.
- **profilePath:** A network path if roaming or mandatory Windows user profiles are being used.

Linux-only Attributes

- **group:** The primary group the user belongs to.
- **logonShell:** The path to the shell process for the user.
- **passwordExpiredDaysBeforeDisabled:** The number of days after the user's password expires that the account is disabled. (N/A in AIX)
- **passwordExpiry:** The date on which the user's account expires and is disabled.
- **passwordExpiryInDays:** The number of days after which the user's password must be changed.
- **passwordMinDaysBetweenChanges:** The minimum number of days permitted between password changes.
- **passwordWarningDays:** The number of days before the user's password is to expire that user is warned.

Short Hand Attributes

- **Standard:** cannotChangePassword, disabled, groups, homeFolder, passwordHasExpired, passwordLastChanged, passwordNeverExpires, user, logonScript (Windows-only), profilePath (Windows-only), group (Unix-only), logonShell (Unix-only), passwordExpiryInDays (Unix-only), passwordMinDaysBetweenChanges (Unix-only)

Meaning of "Key"

The key is the username. This is not a hierarchical EntitySet. Patterns are applied only to the user name. As a result the "**" pattern is not applicable.

The following example monitors for any user creations or deletions. (Note that attributes are explicitly excluded so group membership would not be tracked):

```
<UserSet>
  <Attributes/>
  <include key="*" />
</UserSet>
```

The following example would track the creation and deletion of the "jsmith" account, along with any changes to the STANDARD attributes of the account (since the STANDARD set for this EntitySet is automatically included if no specific attribute list is included):

```
<UserSet>
  <include key="jsmith" />
</UserSet>
```

Sub Elements

Include Exclude

See the general description of include for their allowed attributes and sub elements.

Special attributes of Include/Exclude for UserSets

Various other attributes of the user may be used in include/exclude feature" tests. These tests compare a value against the value of an attribute of the user; take note of the platform support for various attributes - not all attributes are available across platforms or even platform revisions, hence the use of these tests in

© Copyright 2011 Trend Micro Inc.
All rights reserved.

include/exclude elements is of limited use. The feature tests support Unix glob-style wildcarding with * and ?, and there is no normalization of path separators or other characters - it is a simple match against the value of the attribute.

- **Disabled:** Does a true/false match against the disabled attribute of the user. The following example would monitor users with a primary group of either "users" or "daemon":

```
<UserSet>
  <include disabled="true"/>
</UserSet>
```

- **Group:** Does a wildcard match against the primary group of the user. This test is only applicable on Unix systems. The following example would monitor users with a primary group of either "users" or "daemon".

```
<UserSet>
 <include group="users"/>
 <include group="daemon"/>
</UserSet>
```

- **LockedOut:** Does a true/false match against the lockedOut attribute of the user.
- **PasswordHasExpired:** Does a true/false match against the passwordHasExpired attribute of the user.
- **PasswordNeverExpires:** Does a true/false match against the passwordNeverExpires attribute of the user.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

WQLSet

Support for WQLSet elements is available as of DSA 7.0.0.265

The WQLSet element describes a result set from a Windows Management Instrumentation WQL query statement. WQL allows SQL-like queries to be made against many different object classes, with the results forming a table of rows where each row represents an object and each column represents the value of a specific attribute of the object.

Many WMI queries consume a large amount of time and computer resources. It is easy to inadvertently issue a query that takes several minutes to complete and returns thousands of rows. It is highly recommended that all queries be tested before use in a WQLSet using a program like PowerShell or WMI Explorer.

Attribute	Description	Required	Default Value	Allowed Values
namespace	Sets the namespace of the WMI query.	Yes	N/A	String values representing a valid WMI namespace. The "root\cimv2" namespace is the one most commonly used when querying Windows operating system objects, but others such as "root\directory\LDAP" and "root\Microsoft\SqlServer\ComputerManagement" can be used. See here for a small script called GetNamespaces.vbs that enumerates the available WMI namespaces on a given host.
wql	A WQL query string.	Yes	N/A	A valid WQL string. The query must include the __Path attribute for each returned object; the Agent uses the __Path attribute as the entity key when storing and reporting results, so each returned WMI object must include a __Path. If using a query string such as "SELECT * FROM ..." the __Path attribute will be available, but if using a more selective query such as "SELECT Name FROM ..." you must explicitly include __Path by writing the query as "SELECT __Path,Name FROM ...".
onChange	Whether the files returned should be monitored in real time.	No	false	true, false
provider	Optionally specifies an alternative WMI namespace provider to use.	No	none	RsopLoggingModeProvider At present this is only required/supported for group policy queries, and "RsopLoggingModeProvider" is the only supported value. Group policy queries are special since it's recommended that the RsopLoggingModeProvider be used to create a snapshot of the policy data that is present on a computer. If you create a snapshot of the policy data, the query can be performed against a consistent set of data before the system overwrites or deletes it during a refresh of policy. Creating a snapshot actually creates a new WMI namespace, so when using provider="RsopLoggingModeProvider" in a WQLSet, the namespace attribute should specify the suffix to be added to the created namespace. For example, a typical temporary namespace created by the RsopLoggingModeProvider would be "\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010". Specify namespace="Computer" to query "\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010\

© Copyright 2011 Trend Micro Inc.
All rights reserved.

				Computer". Since the temporary namespace is a one-time value, it hampers the ability of the Agent to detect changes since the value appears in the entity key. To avoid this, the Agent will remove the portion of the returned __Path value after \Rsop\ and up to the next backslash when the RsopLoggingModeProvider is used. Entity keys will therefore have prefixes like "\\.\Root\Rsop\Computer" rather than "\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010\Computer"
timeout	Specifies a per-row timeout in milliseconds.	No	5000	1-60000 The WMI query is performed in semisynchronous mode, where result rows are fetched one at a time and there is a timeout on the fetching of a single row. If this parameter is not specified, 5000 (5 seconds) is used as the timeout value.

Entity Set Attributes

Each "row" returned by the WQL query is treated as a single Entity for integrity monitoring purposes, with the returned columns representing the attributes of the entity. Since WMI/WQL is an open-ended specification, there is no set list of available/supported attributes. The query and the schema of the WMI object being queried will determine the attributes being monitored.

For example, the WQLSet:

<WQLSet namespace="Computer" wql="select * from RSOP_SecuritySettings where precedence=1" provider="RsopLoggingModeProvider" />

will return attributes of:

ErrorCode, GPOID, KeyName, SOMID, Setting, Status, id, precedence

whereas a WQLSet that queries network adapters such as:

<WQLSet namespace="root\cimv2" wql="select * from Win32_NetworkAdapter where AdapterTypeId = 0" />

will return attributes such as:

AdapterType, AdapterTypeId, Availability, Caption, ConfigManagerErrorCode, ConfigManagerUserConfig, CreationClassName Description, DeviceID, Index, Installed, MACAddress, Manufacturer, MaxNumberControlled, Name, PNPDeviceID, PowerManagementSupported, ProductName, ServiceName, SystemCreationClassName, SystemName, TimeOfLastReset

In order to reduce the load on the Agent, it is advisable to explicitly include only the attributes that require monitoring rather than use "select * ..." in queries. This also has the benefit that changes to the WMI schema to add or remove attributes will not be reported as changes to the object unless the attributes are part of the set being monitored. With "select * from Win32_Foobar", a patch to Windows that adds a new attribute to the Win32_Foobar object class would result in the next integrity scan reporting a change for every object of that class since a new attribute has appeared.

The following are some example WMI queries which return desirable Windows system entities.

Query for Windows mounted storage devices: (selecting for * will typically result in 80% returned attributes being null or duplicate values)

© Copyright 2011 Trend Micro Inc.
All rights reserved.

<WQLSet namespace="root\cimv2" wql="SELECT __Path,DeviceID,VolumeName,VolumeSerialNumber,DriveType,FileSystem,Access,MediaType,Size,FreeSpace FROM Win32_LogicalDisk" />

To further the preceding query, the DriveType can be specified to isolate only certain types of mounted logical storage devices, such as type 2 which is a "Removable Disk": (like a removable USB storage drive)

<WQLSet namespace="root\cimv2" wql="SELECT __Path,DeviceID,VolumeName,VolumeSerialNumber,DriveType,FileSystem,Access,MediaType,Size,FreeSpace FROM Win32_LogicalDisk WHERE DriveType=2" />

(See here for details on the Win32_LogicalDisk class)

USB Storage Device notes: U3 USB devices will mount both a type 2 "Removable Disk" device and a type 3 "Compact Disc" device. Also, the above query is for storage devices only. USB non-storage devices will not be included. USB memory card adapters may appear as a type 1 "No Root Directory" device. A badly or Windows incompatible USB storage device may appear as a type 1 "Unknown" device.

Query for all known System Directories where the Drive is "F:" for relevant attributes:

<WQLSet namespace="root\cimv2" wql="SELECT __Path,CreationDate,LastAccessed,LastModified,Drive,Path,FileName,Caption,FileType,Readable,Writeable FROM Win32_Directory WHERE Drive='F:'" />

Query for all known System Files where the Drive is 'F:' for relevant attributes:

<WQLSet namespace="root\cimv2" wql="SELECT __Path,CreationDate,LastAccessed,LastModified,Drive,Path,FileName,Name,FileType,Readable,Writeable FROM CIM_DataFile WHERE Drive='F:'" />

Meaning of Key

The key is the "__Path" attribute of the returned WMI object, which is generally of the form:

SystemName\Namespace:WmiObjectClass.KeyAttribute=Value[,KeyAttribute=Value...]

Some examples:

\\TEST-DESK\root\cimv2:Win32_QuickFixEngineering.HotFixID="KB958215-IE7",ServicePackInEffect="SP0"
\\TEST-DESK\ROOT\Rsop\NSF49B36AD_10A3_4F20_9541_B4C471907CE7\Computer:RSOP_RegistryValue.Path="MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\LegalNoticeText",precedence=1
\\TEST-DESK\root\cimv2:BRCM_NetworkAdapter.DeviceID="8"

Sub Elements

Include Exclude

See the general description of "include" and "exclude" for their allowed attributes and sub elements.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

For WQLSet, "include" and "exclude" sub elements should typically not be required. It is preferable to use WQL to specify the exact set of objects to be monitored since that limits the amount of work done by both the Agent and the host's WMI implementation.

The use of any include/exclude sub elements can only reduce the set of objects returned by the query; the WQL must be changed in order to return additional objects. If it is necessary to use include/exclude elements to further restrict the WQL results, "*"and "?" characters can be used as simple wildcards to match against values of the entity key.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Multi-Node Manager

Deep Security Manager can be run as multiple nodes operating in parallel using a single database. Running the Manager as multiple nodes provides increased reliability, redundant availability, virtually unlimited scalability, and better performance.

Each node is capable of all tasks and no node is more important than any of the others. Users can log in to any node to carry out their tasks. The failure of any node cannot lead to any tasks not being carried out. The failure of any node cannot lead to the loss of any data.

Each node must be running the same version of the Manager software. When performing an upgrade of the Manager software, the first Manager to be upgraded will take over all Deep Security Manager duties and shut down all the other Deep Security Manager nodes. They will appear as "offline" in the **Network Map with Activity Graph** in the **System Activity** panel of the **System Information** screen with an indication that an upgrade is required. As the upgrades are carried out on the other nodes, they will automatically be brought back online and begin sharing in the DSM tasks.

Viewing Nodes

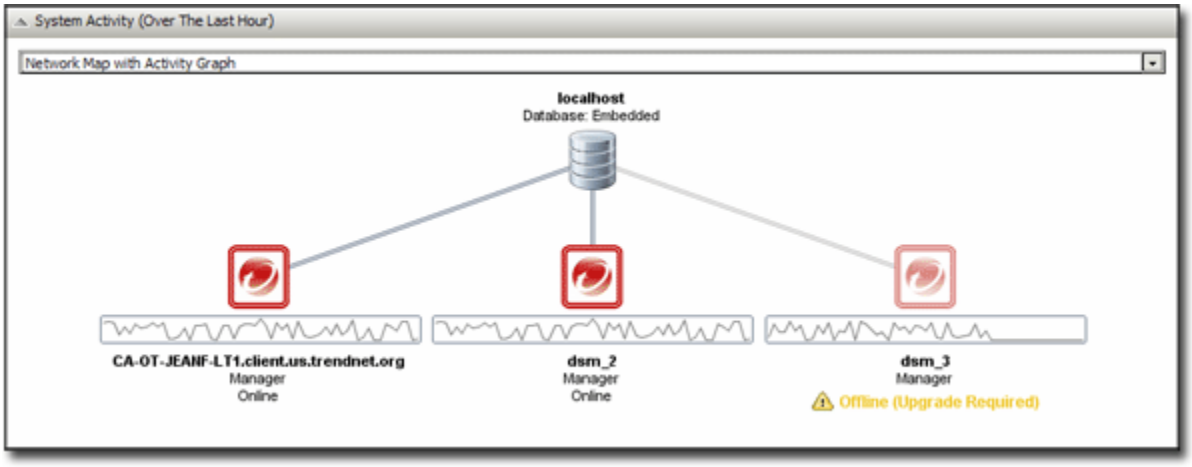
The **Network Map with Activity Graph** in the **System Activity** panel on the **System Information** screen displays all Deep Security Manager nodes along with their status, combined activity and jobs being processed.

The Deep Security Manager processes many concurrent activities in a distributed pool that is executed by all online Manager nodes. All activity not derived from User input is packaged as a job and thus "runnable" on any Manager (with some exceptions for "local" jobs that are executed on each node, like cache clearing).

The Network Map with Activity Graph

The Network Map with Activity Graph displays a map of all installed Manager nodes and their current status as well their relative activity over the last hour. The nodes can be in the following states:

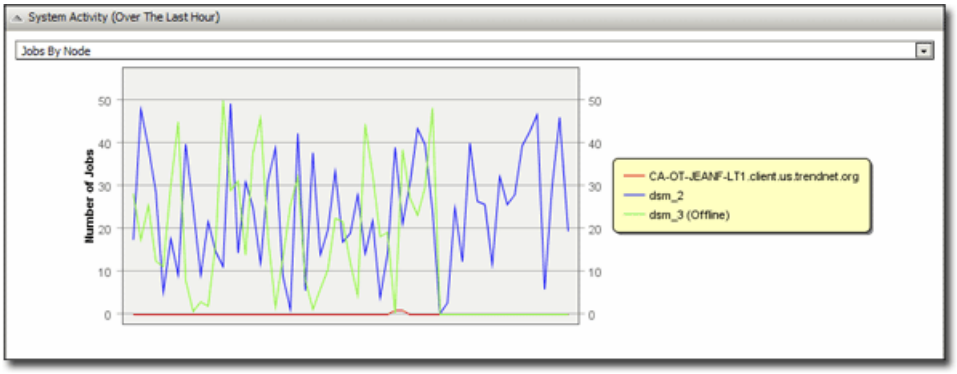
- **Online**
- **Offline**
- **Offline (Upgrade Required)**



© Copyright 2011 Trend Micro Inc.
All rights reserved.

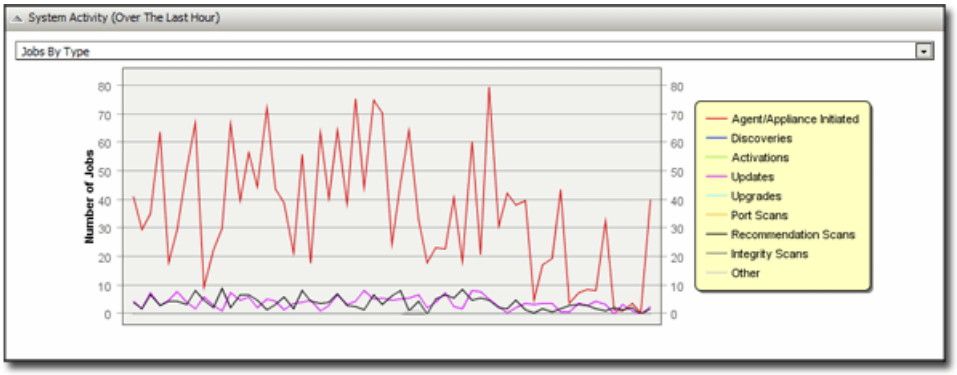
Jobs by Node

This chart breaks down the number of jobs carried out over the last hour by each node.



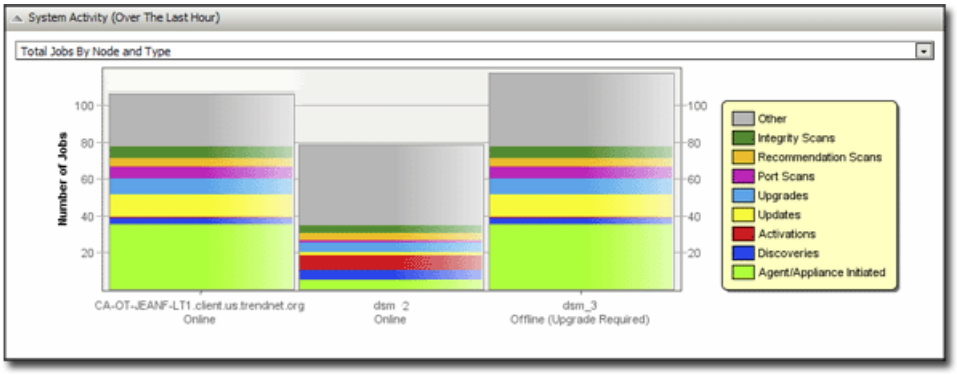
The Jobs by Type

This chart breaks down the jobs carried out over the last hour by type.



Total Jobs by Node and Type

This chart displays the number of job types for each node over the last hour.



© Copyright 2011 Trend Micro Inc.
All rights reserved.

Adding Nodes

To add a Deep Security Manager node to the system, run the Manager install package on a new computer. When prompted, type the location of and login credentials for the database being used. Once the installer connects to the database, you can proceed with adding the node to the system. See the Installation Guide for instructions on adding Deep Security Manager nodes.

Note that you must be using either MS SQL Server or Oracle Database to run multiple nodes.

At no point should more than one instance of the installer be running at the same time. Doing so can lead to unpredictable results including corruption of the database.

Decommissioning Nodes

To decommission a node:

A node must be offline (uninstalled or service halted) to be decommissioned.

1. Click on **Managers...** in the System Information screen toolbar to display the list of Manager nodes.
2. Double click on the Manager node you want to decommission to display its Properties window.
3. Click the **Decommission** button in the **Options** area.

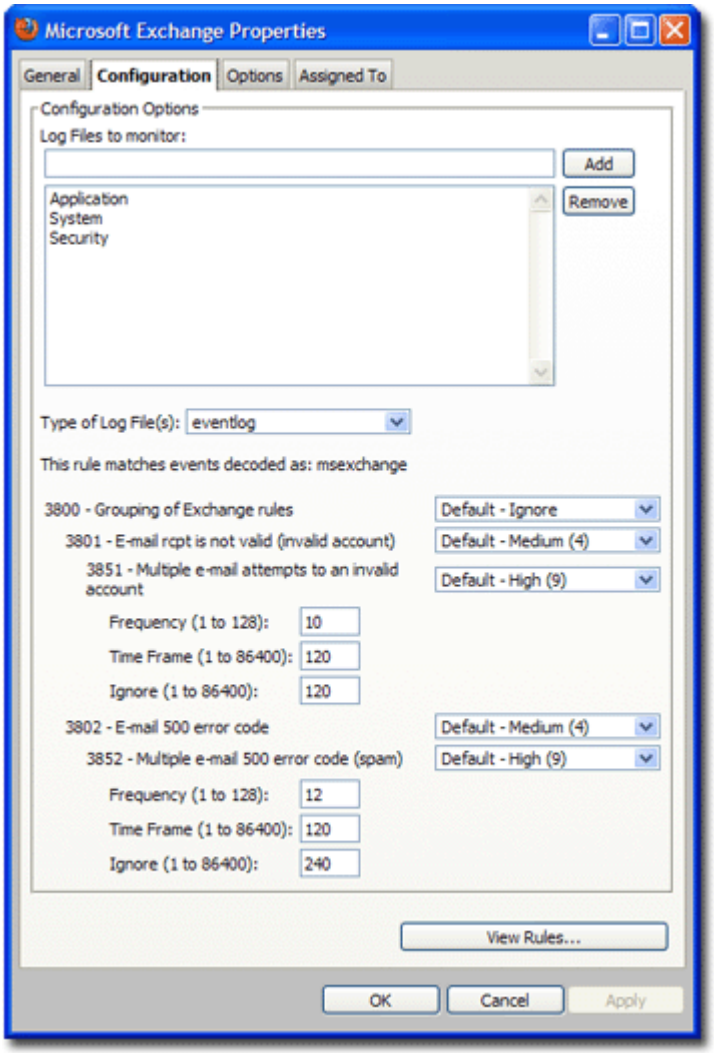
© Copyright 2011 Trend Micro Inc.
All rights reserved.

Options for Log Inspection Rules

The Log Inspection feature in Deep Security enables real-time analysis of 3rd party log files. The Log Inspection Rules and Decoders provide a framework to parse, analyze, rank and correlate events across a wide variety of systems. As with Deep Packet Inspection and Integrity Monitoring, Log Inspection content is delivered in the form of Rules included in a Security Update. These Rules provide a high level means of selecting the applications and logs to be analyzed.

Log Inspection Rule Structure and the Event Matching Process

This screen shot displays the contents of the **Configuration** tab of the Properties window of the "Microsoft Exchange" Log Inspection Rule:



© Copyright 2011 Trend Micro Inc.
All rights reserved.

Here is the structure of the Rule:

```
3800 - Grouping of Exchange Rules - Ignore
   3801 - Email rcpt is not valid (invalid account) - Medium (4)
      3851 - Multiple email attempts to an invalid account - High
(9)
         Frequency - 10
         Time Frame - 120
         Ignore - 120
   3802 - Email 500 error code - Medium (4)
      3852 - Email 500 error code (spam) - High (9)
         Frequency - 12
         Time Frame - 120
         Ignore - 240
```

The Log Inspection engine will apply Log Events to this structure and see if a match occurs. Let's say that an Exchange event occurs, and this event is an email receipt to an invalid account. The event will match line 3800 (because it is an Exchange event). The event will then be applied to line 3800's sub-rules: 3801 and 3802.

If there is no further match, this "cascade" of matches will stop at 3800. Because 3800 has a severity level of "Ignore", no Log Inspection Event would be recorded.

However, an email receipt to an invalid account does match one of 3800's sub-rules: sub-rule 3801. Sub-rule 3801 has a severity level of "Medium(4)". If the matching stopped here, a Log Inspection Event with a severity level of "Medium(4)" would be recorded.

But there is still another sub-rule to be applied to the event: sub-rule 3851. Sub-rule 3851 with its three attributes will match if the same event has occurred 10 times within the last 120 seconds. If so, a Log Inspection Event with a severity "High(9)" is recorded. (The "Ignore" attribute tells sub-rule 3851 to ignore individual events that match sub-rule 3801 for the next 120 seconds. This is useful for reducing "noise".)

Assuming the parameters of sub-rule 3851 have been matched, a Log Inspection Event with Severity "High(9)" is now recorded.

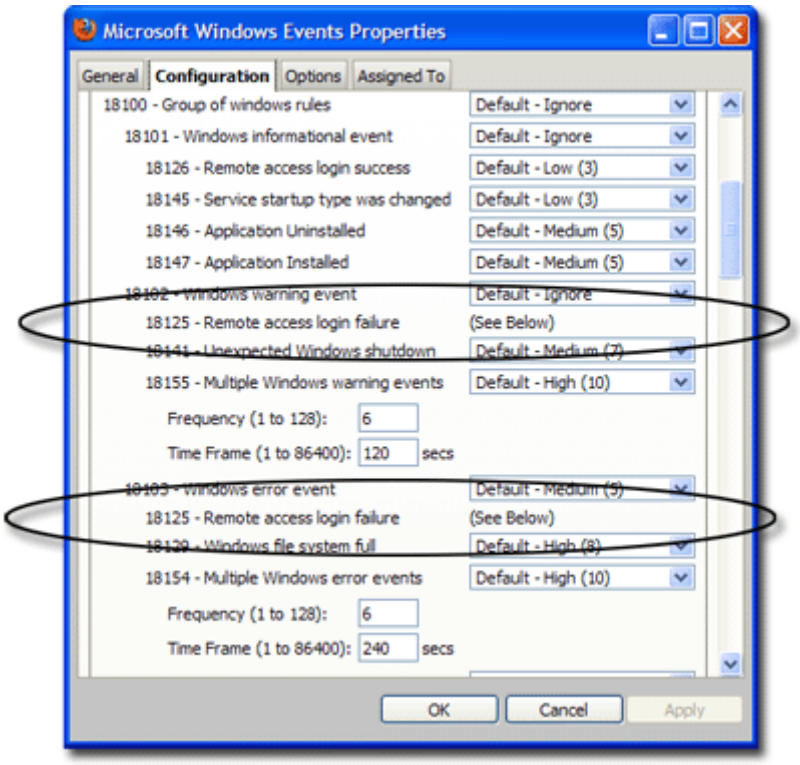
Looking at the Options tab of the Microsoft Exchange Rule, we see that Deep Security Manager will raise an Alert if any sub-rules with a severity level of "Medium(4)" have been matched. Since this is the case in our example, the Alert will be raised (if "Alert when this rule logs an event" is selected).

Duplicate Sub-rules

Some Log Inspection Rules have duplicate sub-rules. To see an example, open the "Microsoft Windows Events" rule and click on the **Configuration** tab. Note that sub-rule 18125 (Remote access login failure) appears under sub-rules 18102 and 18103. Also note that in both cases sub-rule 18125 does not have a severity value, it only says "See Below".

Instead of being listed twice, Rule 18125 is listed once at the bottom of the **Configuration** page:

© Copyright 2011 Trend Micro Inc.
All rights reserved.



Conclusion

By adjusting the severity levels of the different sub-rules you can:

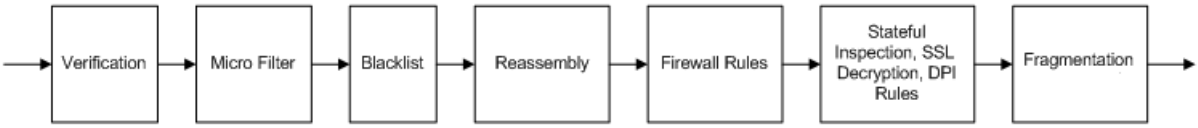
- Collect more events (Change the base "Ignores" to a severity 1-15)
- Tune down specific events you are not interested in
- Tune up specific events you are more interested in or want to alert on

The additional configuration options provided in Security Update 09-004 provide a rich way to configure the Log Inspection Rules and provide visibility into the sub-rules, letting Users create additional chains off the existing rules.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

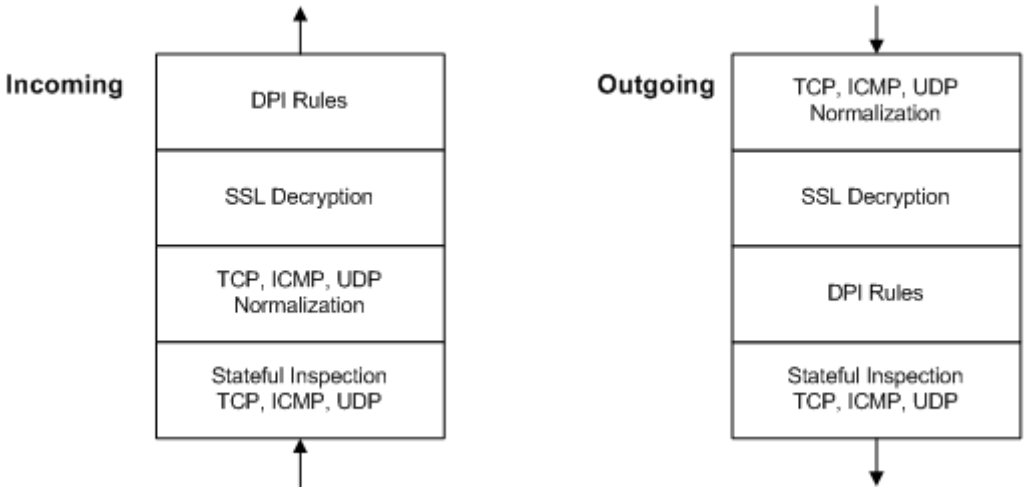
Packet Processing Sequence

Both incoming and outgoing network traffic gets fed through a pipeline of modules:



- **Verification:** Basic checks for validity of the packet
- **Micro Filter:** Basic firewall bypass rules are enforced at this layer
- **Blacklist:** Maintains a list of known bad IPs as used by the Traffic Analysis feature
- **Fragmentation:** Fragments packets that are larger than the MTU
- **Firewall Rules :** All packets not processed by the Micro Filter are processed by the Firewall
- **Stateful Inspection, SSL Decryption, and DPI Rules:** Acts as one module where the following functions are performed:
  - **Stateful Inspection:** Maintains known connections that are valid for a response. This feature also controls the connection limits and does SYN Flood and ACK Storm protection
  - **SSL Decryption:** If required and configured this feature decrypts the SSL protected traffic for analysis by the DPI engine
  - **DPI:** Deep Packet Inspection engine that does pattern matching and custom code operations
- **Reassembly:** Reassembles fragmented packets for later use by the DPI engine

Although incoming and outgoing traffic flow through the pipeline in the same order, the internal sub-order inside the **Stateful Inspection, SSL, and DPI** module depends on traffic direction:



© Copyright 2011 Trend Micro Inc.
All rights reserved.

Ports Used by Deep Security

A number of ports must be accessible for the Deep Security Manager and the Agents/Appliances to function as expected. The following is a list of the ports used, the description of the function for which the port is used, the related protocols, the application which initializes the connection, the application to which the connection is made, whether the use of a proxy is possible (and what type of proxy), and whether and where the port can be configured:

Port: 4118

- Use: Manager-to-Agent/Appliance communication.
- Protocol: TCP
- Initiated By: Deep Security Manager
- Connected To: Agent/Appliance
- Proxy: No
- Configuration: This port is not configurable (please contact your support provider if this port assignment is problematic.)

Port: 4119 (default)

- Use:
  - Access to Deep Security Manager Web browser interface.
  - Access to Deep Security Manager by an ESX server to request the Deep Security Filter Driver during the preparation of an ESX server for Anti-Malware protection.
  - Requests for security updates by the Deep Security Virtual Appliance.
- Protocol: TCP
- Initiated By:
  - Web Browser
  - ESX server
  - Deep Security Virtual Appliance
- Connected To: Deep Security Manager
- Proxy: No
- Configuration: This port is configured during the Deep Security Manager installation process.

Port: 4120 (default)

- Use: Agent/Appliance-to-Manager communication
- Protocol: TCP
- Initiated By: Agent/Appliance
- Connected To: Deep Security Manager
- Proxy: No
- Configuration: This port is configured during the Deep Security Manager installation process.

Port: 514 (default)

- Use: Syslog
- Protocol: UDP
- Initiated By: Agent/Appliance
- Connected To: Syslog facility
- Proxy: No
- Configuration: This port can be configured in **System > System Settings > Notifications**.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Port: 25 (default)

- Use: E-mail Alerts
- Protocol: TCP
- Initiated By: Deep Security Manager
- Connected To: Specified SMTP server
- Proxy: No
- Configuration: This port can be configured in **System > System Settings > System**.

Port: 80

- Use: Connection to Trend Micro ActiveUpdate Server
- Protocol: HTTP and SOCKS
- Initiated By: Deep Security Manager
- Connected To: Trend Micro ActiveUpdate Server
- Proxy: Yes (optional)
- Configuration: The proxy address and port can be configured in **System > System Settings > Updates**.

Port: 389

- Use: LDAP directory addition or Deep Security Manager
- Protocol: TCP
- Initiated By: Deep Security Manager
- Connected To: LDAP server
- Proxy: No
- Configuration: This port can be configured in the **New Directory** wizard.

Port: Randomly selected

- Use: DNS lookup for hostnames
- Protocol: TCP
- Initiated by: Deep Security Manager
- Connected to: DNS server
- Proxy: No
- Configuration: The port is randomly selected when the Deep Security Manager needs to lookup a hostname.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Protecting a Mobile Laptop

In this guide, we will use the Manager to protect a mobile laptop. This will involve the following steps:

1. Adding Computers to the Manager
    a. Adding individual computers
    b. Performing a Discovery Operation on your network
    c. Importing computers from a Microsoft Active Directory
2. Create a new Security Profile for a Windows laptop
    a. Creating and naming the new Security Profile
    b. Setting which interfaces to monitor
    c. Setting the network engine to Inline Mode
    d. Assigning Firewall Rules (including some with Location Awareness) and enabling Stateful Configuration
    e. Assigning Deep Packet Inspection (DPI) Rules
    f. Assigning Log Inspection Rules
    g. Assigning Integrity Monitoring Rules
3. Applying the Security Profile to the computer
4. Monitoring Activity using the Manager

We will assume that you have already installed the Manager on the computer from which you intend to manage the Deep Security Agents throughout your network. We will also assume that **you have installed (but not activated) Deep Security Agents on the mobile laptops you wish to protect**. If you have not done so, consult the installation instructions for the steps to get to this stage.

Adding computers to the Manager

There are four ways of adding computers to the Deep Security **Computers** screen:

1. Adding computers individually by specifying their IP addresses or hostnames
2. Discovering computers by scanning the network
3. Connecting to a Microsoft Active Directory and importing a list of computers
4. Connecting to a VMware vCenter and importing a list of computers (not covered in this article because we are dealing with mobile laptops.)

Adding computers individually by specifying their IP addresses or hostnames

To add an individual computer by specifying its IP address or hostname, go to the **Computers** screen by clicking **Computers** in the navigation pane and click **New** in the toolbar.

Type the hostname or IP address of the new computer in the **Hostname** textbox. The **New Computer** wizard also lets you specify a Security Profile which it will apply to the new computer if it finds the computer and determines that an unactivated Agent is present. (For now, don't select a Security Profile.) When you click **Next**, the wizard will find the computer and activate the Agent. When Agent activation has completed, the wizard will give you the option of opening the computer's **Details** screen which lets you configure many the Agent's settings. Skip the **Details** screen for now.

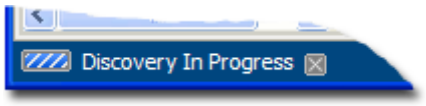
Adding computers by scanning the network (Discovery)

To discover computers by scanning the network:

1. Go to the **Computers** screen by clicking **Computers** in the navigation pane.
2. Click **Discover...** in the toolbar to display the **Discover Computers** dialog box.
3. Type a range of IP addresses you want to scan for computers. If you wish, you can enter a masked IP address to do the same thing.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

4. Select **Automatically resolve IPs to hostnames** to instruct the Manager to automatically resolve hostnames as it performs the discovery.
5. You have the option to add discovered computers to a computer group you have created. For now, leave the **Add Discovered Computers to Group** drop-down list choice set to "Computers".
6. Finally, clear the **Automatically perform a port scan of discovered computers** checkbox. (Port scanning detects which ports are open on the discovered computers.)
7. Click **OK**. The dialog box will disappear and "Discovery in progress..." will appear in the Manager's status bar in the bottom left corner of your browser. (The discovery process can be cancelled by clicking the "X".)



In a few minutes, all visible computers on the network will have been detected and the Manager will have identified those with Deep Security Agents installed. These Agents now need to be activated.

8. Activate the Agents by right-clicking an Agent (or multiple selected Agents), and select "Activate/Reactivate" from the shortcut menu. Once the Agents are activated, their status light will turn green and "Managed (Online)" will appear in the status column.

Importing Computers from a Microsoft Active Directory

Computers imported from an Active Directory are treated the same as any other computers in the **Computers** screen.

To import computers from a Microsoft Active Directory:

1. Click the down arrow next to "New" in the **Computers** screen toolbar and select **Add Directory...**. to start the **Add Directory** wizard.

Other LDAP-based directories are supported but require some customization. For assistance please contact your support provider.

2. Type the Active Directory server name, a name and description for your imported directory as it will appear in the Manager (it doesn't have to match that of the Active Directory), the IP and port of the Active Directory server, and finally your access method and credentials. Click **Next**.

Note that you must include your domain name with your username in the **User Name** field.

3. If you select SSL or TLS as the Access method, the wizard will ask you to accept a security certificate. You can view the certificate accepted by the Deep Security Manager by going to **System > System Settings > Security** and clicking "View Certificate List..." in the Trusted Certificates area. Click **Next**.
4. The second screen of the **New Directory** wizard asks for schema details. (Leave the default values). Click **Finish**.
5. The next screen will tell you if there were any errors. Click **Next**.
6. The final screen will let you create a Scheduled Task to regularly synchronize the Manager's **Computers** screen with the Active Directory. Leave option this cleared for now. Click **Close**.

The directory structure now appears under **Computers** in the Navigation pane.

Additional Active Directory Options

Right-clicking an Active Directory structure gives you the following options that are not available for ordinary computer groups listed under **Computers**.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

1. Remove Directory
2. Synchronize Now

Remove Directory

When you remove a directory from the Deep Security Manager, you have the following options:

- **Remove directory and all subordinate computers/groups from DSM:** removes all traces of the directory.
- **Remove directory, but retain computer data and computer group hierarchy:** turns the imported directory structure into identically organized regular computer groups, no longer linked with the Active Directory server.
- **Remove directory, retain computer data, but flatten hierarchy:** removes links to the Active Directory server, discards directory structure, and places all the computers into the same computer group.

Synchronize Now

Synchronizes the directory structure in the Deep Security Manager with the Active Directory Server. (Remember that you can automate this procedure as a **Scheduled Task**.)

Now that the Agents are active, they can be assigned Firewall Rules and DPI Rules. Although all the individual security elements can be assigned individually to an Agent, it is convenient to group common security elements into a Security Profile and then assign the Security Profile to one or more Agents.

More information is available for each screen in the Deep Security Manager by clicking the **Help** button in the menu bar.

Activating the Agents on Computers

Agents need to be "activated" by the Manager before rules can be assigned to them. The activation process includes the exchange of unique fingerprints between the Agent and the Manager. This ensures that only this Deep Security Manager (or one of its nodes) can send instructions to the Agent.

Computers that are added individually to the **Computers** list have their Agents activated automatically. Computers that are added to the **Computers** screen by the discovery process and those imported from an Active Directory or VMware vCenter must be activated manually.

To manually activate an Agent on a computer, right-click one or more selected computers, go to "Actions" and select "Activate/Reactivate".

Create a Security Profile for a Windows laptop

Now that the Agents are activated, it's time to assign some rules to protect the computer. Although you can assign rules directly to a computer, it's more useful to create a Security Profile which contains these rules and which can then be assigned to multiple computers.

Creating the Security Profile will involve the following steps:

1. Creating and naming the new Security Profile
2. Setting which interfaces to monitor
3. Setting the network engine to Inline Mode
4. Assigning Firewall Rules (including some with location awareness) and enable Stateful Inspection
5. Assigning Deep Packet Inspection (DPI) Rules
6. Assigning Integrity Monitoring Rules
7. Assigning Log Inspection Rules
8. Assigning the Security Profile to the computer

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Creating and naming the New Security Profile

To create and name the new Security Profile:

1. Click **Security Profiles** in the Manager's navigation pane, and then click **New** to display the **New Security Profile** wizard.
2. Name the new Security Profile "My New Laptop Security Profile". Click **Next.**
3. The next screen asks if you would like to base the Security Profile on an existing computer's current configuration. If you were to select **Yes**, you would be asked to pick an existing managed computer and the wizard would take all the configuration information from that computer and create a new Security Profile based on it. This can be useful if, for instance, you have fine-tuned the security configuration of an existing computer over a period of time and now wish to create a Security Profile based on it so that you can apply it to other functionally identical computers. For now, select **No** and click **Next**.
4. The last screen confirms that the new Security Profile has been created. Select the **Open Security Profile Details on 'Close'** option and click **Close**.

Setting which interfaces to monitor

To set which interfaces to monitor:

1. Because you set the **Open Security Profile Details on 'Close'** option, the new Security Profile's **Details** screen is displayed.
2. The laptops to which this Security Profile will be assigned are equipped with two network interfaces (a local area connection and a wireless connection) and we intend to tune the security configuration to take into account which interface is being used. Click **Interface Types** in the navigation pane and select the **Multiple Interface Types** option. Type names for the interfaces and strings (with optional wildcards) which the Agent will use to match interface names on the computer: "LAN Connection" and "Local Area Connection *", and "Wireless" and "Wireless Network Connection *" in the first two Interface Type areas. Click **Save** at the bottom right of the screen.

Setting the network engine to Inline Mode

The Agent's network engine can operate Inline or in Tap Mode. When operating Inline, the live packet stream passes through the network engine. Stateful tables are maintained, Firewall Rules are applied and traffic normalization is carried out so that DPI Rules can be applied to payload content. When operating in Tap Mode, the live packet stream is cloned and diverted from the main stream. In Tap Mode, the live packet stream is not modified; all operations are carried out on the cloned stream.

For now, we will configure our Security Profile to direct the engine to operate Inline.

To set the network engine to Inline Mode:

1. Still in the My New Laptop Security Profile **Details** screen, go to **System > System Settings** and click on the **Firewall and DPI** tab.
2. Set the Network Engine Mode to **Inline**. By default, the setting should already be set to "Inherited (Inline)" since the global default mode (configured in the main Deep Security Manager system settings) is **Inline** and new Security Profiles inherit global settings.

Assigning Firewall Rules (including some with location awareness) and turn on Stateful Inspection

To assign Firewall Rules:

1. Click **Firewall** in the navigation pane, de-select the **Inherit** checkbox and select **On** beneath it.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

The "Inherit" checkbox determines whether or not these settings will be inherited from global settings defined in the Manager. For information on Inheritance, see "Inheritance and Overrides" in the **Reference** section.

2. Now we will assign some Firewall Rules and Stateful Configuration rules to this Security Profile. Click **Firewall Rules** to display the list of available predefined Firewall Rules. (You can create your own Firewall Rules, but for this exercise we will select from the list of existing ones.) Select the following set of Firewall Rules to allow basic communication:

   - Allow Solicited ICMP replies
   - Allow solicited TCP/UDP replies
   - Domain Client (UDP)
   - ARP
   - Wireless Authentication
   - Windows File Sharing (This is a force-allow rule to permit incoming Windows File Sharing traffic.)

   Notice the gray down-arrow next to the Firewall Rule checkboxes. These appear if you have defined multiple interfaces in the previous step. They allow you to specify whether the Firewall Rule will apply globally to all interfaces on the computer or just to interfaces that you specify. Leave these at the default setting for now. Click the **Save** button.

We assigned a Firewall Rule that permitted Windows File Sharing. Windows File Sharing is a very useful feature in Windows but it has had some security issues. It would better to restrict this ability to when the laptop is in a secure office environment and forbid it when the laptop is out of the office. We will apply Location Awareness to the Firewall Rule when used with this Security Profile to implement this policy.

To implement location awareness:

1. In the **My New Laptop Security Profile** Security Profile **Details** screen, right-click the Windows File Sharing Firewall Rule and select **Properties (for this Security Profile)**. This will display the **Properties** window for the Firewall Rule (but the changes we make to it will only apply to the Firewall Rule when it is applied as part this new Security Profile).
2. In the **Properties** window, click the **Options** tab.
3. In the **Rule Context** area, select **New...** from the drop-down list. This displays the **New Context** Properties window. We will create a Rule Context that will only allow the Firewall Rule to be active when the laptop has local access to its Domain Controller. (That is, when the laptop is in the office.)
4. Name the new Rule Context "In the Office". In the **Options** area, set the **Perform check for Domain Controller connectivity** option and select **Local** below it. Then click **Ok**.
5. Click **OK** in the Windows File Sharing Firewall Rule **Properties** window.

Now the Windows File Sharing Firewall Rule will only be in effect when the laptop has local access to its Windows Domain Controller. The Windows File Sharing Firewall Rule is now displayed in bold letters in the Security Profile **Details** screen. This indicates that the Firewall Rule has had its properties edited for this Security Profile only.

Note that Location Awareness is also available for DPI Rules.

The final step in the Firewall section is to enable Stateful inspection.

To enable Stateful Inspection:

1. Still in the **My New Laptop Security Profile** Security Profile **Details** screen, click **Stateful Configurations** under Firewall in the navigation pane.
2. Under "Global (All Interfaces)" select "Enable Stateful Inspection".
3. Click **Save** to finish.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Assigning Deep Packet Inspection (DPI) Rules

To assign Deep Packet Inspection (DPI) rules to the Security Profile:

1. Still in the "My New Laptop Security Profile" **Details** window, click **Deep Packet Inspection** in the navigation pane.
2. In the **Deep Packet Inspection** area, clear the **Inherit** check box, and select **On** beneath it.

DPI can be set to either Prevent or Detect mode when the Network Engine is operating Inline (as opposed to Tap Mode). Detect mode is useful if you are trying out a new set of DPI Rules and do not want to risk dropping traffic before you are sure the new rules are working properly. In Detect Mode, traffic that would normally be dropped will generate events but will be allowed to pass. Set Deep Packet Inspection to "On".

Note the **Recommendations** area. The Deep Security Agent can be instructed to run a Recommendation Scan. (On the Manager's **Computers** screen, right-click a computer and select **Actions > Scan for Recommendations.**) The Recommendation engine will scan the computer for applications and make DPI Rule recommendations based on what it finds. The results of the Recommendation Scan can be viewed in the computer's **Details** window by clicking **Deep Packet Inspection > DPI Rules** and selecting "Show Recommended" from the **Show** drop-down list.

3. For now, leave the **Recommendations** option set to **Inherited (No)**.
4. DPI Rules are organized by Application Type. Application Types are a useful way of grouping DPI Rules; they have only three properties: communication direction, protocol, and ports. For our new laptop Security Profile, assign the following Application Types:
    - Mail Client Outlook
    - Mail Client Windows
    - Malware
    - Malware Web
    - Microsoft Office
    - Web Client Common
    - Web Client Internet Explorer
    - Web Client Mozilla Firefox
    - Windows Services RPC Client
    - Windows Services RPC Server
5. Click **DPI Rules** under **Deep Packet Inspection** in the navigation pane. Sort the DPI Rules "By Application Type" and then put a check next to the Application Types listed above. (There are many Application Types and DPI Rules, so you will have to have to use the pagination controls at the bottom right of the screen to get to them all, or use the search features at the top right of the screen.)

Some DPI Rules are dependent on others. If you assign a rule that requires another rule to also be assigned (which has not yet been assigned) a popup window will appear letting you assign the required rule.

When assigning any kinds of Rules to a computer, do not let yourself be tempted to be "extra secure" and assign all available rules to your computer. The Rules are designed for a variety of operating systems, applications, vulnerabilities and may not be applicable to your computer. The traffic filtering engine would just be wasting CPU time looking for patterns that will never appear. Be selective when securing your computers!

6. Click **Save** to assign the Application Types to the Security Profile.

Assigning Integrity Monitoring Rules

To assign Integrity Monitoring Rules to the Security Profile:

1. Still in the "My New Laptop Security Profile" **Details** window, click "Integrity" in the navigation pane.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

2. Deselect the **Inherit** option and set Integrity to **On**.
3. Set **Automatically assign recommended Integrity Monitoring Rules to Computer during Recommendation Scans** to **No**.
4. Now click **Integrity Monitoring Rules** under **Integrity Monitoring** in the navigation pane.
5. In the Search box at the top right of the screen type the word "Windows" and press Enter. All the rules that apply to Microsoft Windows will be displayed in the rules list. Right-click one of the rules and choose "Select All", then right-click again and choose "Assign Rule(s)". This will assign all the rules that came up in the search result to the Security Profile.

Assigning Log Inspection Rules

To assign Log Inspection Rules to the Security Profile:

1. Still in the "My New Laptop Security Profile" **Details** window, click **Log Inspection** in the navigation pane.
2. Deselect **Inherit** and set Log Inspection to **On**.
3. Set **Automatically assign recommended Log Inspection Rules to Computer during Recommendation Scans** to **No**.
4. Go to the **Log Inspection > Log Inspection Rules** screen and select the "1002792 - Default Rules Configuration" Rule (required for all other Log Inspection Rules to work), and the "1002795 – Microsoft Windows Events" rule. (This will log events any time Windows auditing functionality registers an event on the laptop.)
5. Click **Save** to apply the rules to the Security Profile.

We are now finished editing the new Security Profile. You can now close the My New Security Profile **Details** screen.

Edit the Domain Controller(s) IP List

Finally, since the new Security Profile includes three Firewall Rules that use the "Domain Controller(s)" IP List, we will have to edit that IP List to include the IP addresses of the local Windows Domain Controller.

To edit the Domain Controllers IP list:

1. In the main window of the Manager, go to the **Components > IP Lists**.
2. Double-click the **Domain Controller(s)** IP List to display its **Properties** window.
3. Type the IP(s) of your domain controller(s).
4. Click **OK**.

Apply the Security Profile to a Computer

Now we can apply the Security Profile to the computer.

To apply the Security Profile to the computer:

1. Go to the **Computers** screen.
2. Right-click the computer to which you will assign the Security Profile and select **Actions > Assign Security Profile...**.
3. Choose "My New Laptop Security Profile" from the drop-down list in the **Assign Security Profile** dialog box.
4. click **OK**

After clicking **OK**, the Manager will send the Security Profile to the Agent. The computer **Status** column and the Manager's status bar will display messages that the Agent is being updated.

Once the Agent on the computer has been updated, the **Status** column will read "Managed (Online)".

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Configure SMTP Settings

Configuring the Deep Security Manager's SMTP settings allows email alerts to be sent out to Users.

To configure SMTP settings:

1. Go to **System > System Settings** and click the **System** tab.
2. Type the configuration information and click the **Test SMTP Settings** to confirm Deep Security Manager can communicate with the mail server.
3. Click the **Notifications** tab.
4. On the **Notifications** screen, type the default email address to which you want notifications sent.
5. Click **Save**.

Whether a User gets emailed alerts can be configured on that User's **Properties** window (**System > Users**). Whether a particular Alert generates emailed notifications can be configured on that Alert's **Properties** window (**System > System Settings > System > View Alert Configuration...**).

Monitor Activity Using the Deep Security Manager

The Dashboard

After the computer has been assigned a Security Profile and has been running for a while, you will want to review the activity on that computer. The first place to go to review activity is the Dashboard. The Dashboard has many information panels ("widgets") that display different types of information pertaining to the state of the Deep Security Manager and the computers that it is managing.

At the top right of the Dashboard screen, click **Add/Remove Widgets** to view the list of available widgets.

For now, we will add the following widgets from the **Firewall** section:

- Firewall Activity (Prevented)
- Firewall IP Activity (Prevented)
- Firewall History (2x1)

Select the checkbox beside each of the three widgets, and click **OK**. The widgets will appear on the dashboard. (It may take a bit of time to generate the data.)

- The **Firewall Activity (Prevented)** widget displays a list of the most common reasons for packets to be denied (that is, blocked from reaching a computer by the Agent on that computer) along with the number of packets that were denied. Items in this list will be either types of Packet Rejections or Firewall Rules. Each "reason" is a link to the corresponding logs for that denied packet.
- The **Firewall IP Activity (Prevented)** widget displays a list of the most common source IPs of denied packets. Similar to the **Firewall Denied Activity** widget, each source IP is a link to the corresponding logs.
- The **Firewall History (2x1)** widget displays a bar graph indicating how many packets were blocked in the last 24 hour period or seven day period (depending on the view selected). Clicking a bar will display the corresponding logs for the period represented by the bar.

Note the trend indicators next to the numeric values in the **Firewall Denied Activity** and **Firewall IP Activity (Denied)** widgets. An upward or downward pointing triangle indicates an overall increase or decrease over the specified time period, and a flat line indicates no significant change.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Logs of Firewall and DPI Events

Now drill-down to the logs corresponding to the top reason for Denied Packets: in the **Firewall Denied Activity** widget, click the first reason for denied packets (in the picture above, the top reason is "Out of Allowed Policy"). This will take you to the **Firewall Events** screen.

The **Firewall Events** screen will display all Firewall Events where the **Reason** column entry corresponds to the first reason from the **Firewall Denied Activity** widget ("Out of Allowed Policy"). The logs are filtered to display only those events that occurred during the view period of the Dashboard (Last 24 hours or last seven days). Further information about the **Firewall Events** and **DPI Events** page can be found in the help pages for those screens.

For the meaning of the different packet rejection reasons, see Firewall Events and DPI Events.

Reports

Often, a higher-level view of the log data is desired, where the information is summarized, and presented in a more easily understood format. The **Reports** fill this role, allowing you to display detailed summaries on computers, Firewall and DPI Event Logs, Events, Alerts, etc. In the **Reports** screen, you can select various options for the report to be generated.

We will generate a **Firewall Report**, which displays a record of Firewall Rule and Stateful Configuration activity over a configurable date range. Select **Firewall Report** from the Report drop-down. Click **Generate** to launch the report in a new window.

By reviewing scheduled reports that have been emailed by the Deep Security Manager to Users, by logging into the system and consulting the dashboard, by performing detailed investigations by drilling-down to specific logs, and by configuring alerts to notify Users of critical events, you can remain apprised of the health and status of your network.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Recommendation Scans

When you instruct Deep Security to run a Recommendation Scan on a computer, the Deep Security Agent scans the computer's registry, running processes, open ports, file system, and services for known vulnerabilities. The Agent scans not only the operating system but also installed applications. Based on what is detected, Deep Security will recommend DPI Rules, Log Inspection Rules, and System Integrity Rules.

For large deployments, Trend Micro recommends managing Recommendations at the Security Profile level. That is, all computers that are to be scanned should already have a Security Profile assigned to them. This way, you can make all your rule assignments from a single source (The Security Profile) rather than having to manage individual rules on individual computers.

Recommendation Scans can be initiated manually or you can create a Scheduled Task to periodically run scans on certain computers.

To launch a Recommendation Scan manually:

1. In the Deep Security Manager, go to the **Computers** screen.
2. Select the computer or computers you want to scan.
3. Right-click the selection and choose **Actions > Scan for Recommendations**.

To create a Recommendation Scan Scheduled Task:

1. In the Deep Security Manager, go to the **System > Tasks** screen.
2. Click **New** on the toolbar and select 'New Scheduled Task" to display the **New Scheduled Task** wizard.
3. Select "Scan Computers for Recommendations" from the **Type** menu and select how often you want the scan to occur. Click **Next**.
4. The next screen will let you be more specific about the scan frequency, depending on your choice in step 3. Make your selection and click **Next**.
5. Now select which computer(s) will be scanned and click **Next**.

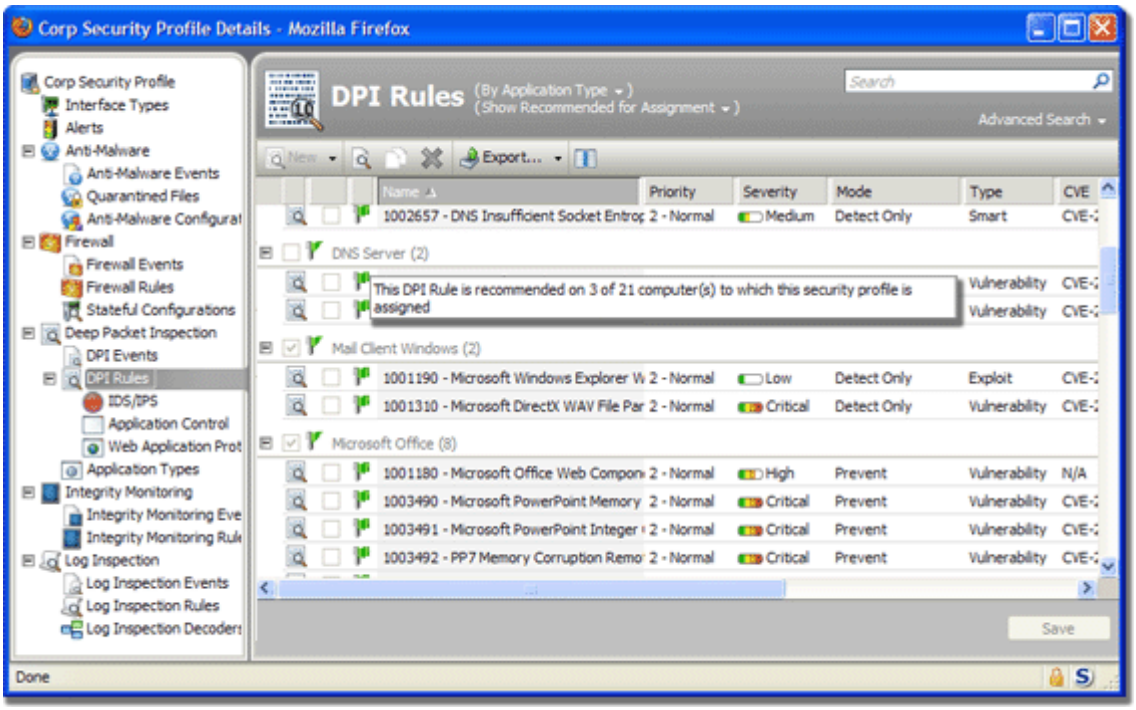
As usual, for large deployments it's best to perform all actions through Security Profiles.

6. Finally, give a name to your new Scheduled Task, select whether or not to "Run Task on 'Finish'", click **Finish**.

Managing Recommendation Scan Results

Once a Recommendation Scan is complete, open the Security Profile that is assigned to the computers you have just scanned. Navigate to **Deep Packet Inspection > DPI Rules**. Sort the rules "By Application Type", and select "Show Recommended for Assignment" from the display filter menu:

© Copyright 2011 Trend Micro Inc.
All rights reserved.



All the recommendations made for all the computers included in the Security Profile will be listed.

Note that there are two kinds of green flags. Full flags ( ) and partial flags( ). Recommended Rules always have a full flag. Application Types may have a full or partial flag. If the flag is full, it signifies that all the Rules that are part of this Application Type have been recommended for assignment. If the flag is partial, it signifies that only some of the Rules that are part of this Application Type have been recommended.

Also notice the tool tip in the screen shot above. It reads: "This DPI Rule is recommended on 3 of 21 computer(s) to which the security profile is assigned." Trend Micro recommends assigning all the recommended Rules to all the computers covered by the Security Profile. This may mean that some Rules are assigned to computers on which they are not required. However, the minimal effect on performance is outweighed by the ease of management that results from working through Security Profiles.

Remember that a Recommendation Scan will make recommendations for DPI Rules, Log Inspection Rules, and Integrity Monitoring Rules.

Once a Recommendation Scan has run, Alerts will be raised on the all computers for which recommendations have been made.

The results of a recommendation scan can also include recommendation to unassign rules. This can occur if applications are uninstalled, if security patches from a manufacturer are applied, or if unnecessary rules have been applied manually. To view rules that are recommended for unassignment, select "Show Recommended for Unassignment" from the display filter menu.

Configuring Recommended Rules

Some Rules require configuration before they can be applied. For example, some Log Inspection Rules require that you specify the location of the log files to be inspected for change. If this is the case, an Alert will be raised on the Computer on which the recommendation has been made. The text of the Alert will contain the information required to configure the rule.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Role-Based Access Control

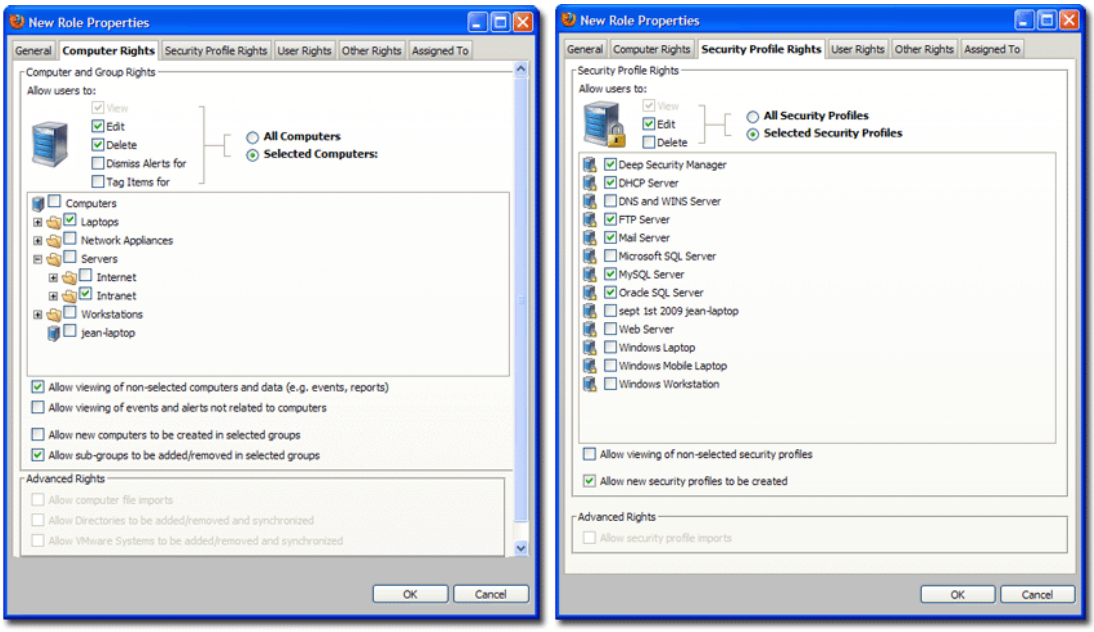
The following features allow the creation of Roles that have exclusive access to certain areas of Deep Security such as computer groups, Security Profiles, Firewall Rules, Stateful Configurations, DPI Rules, and system settings.

Role-Based Access Rights and Editing Privileges

Access rights and editing privileges are attached to Roles and not to Users. To change the access rights and editing privileges of an individual User, the User must be assigned a different role, or the role itself must be edited.

Role-Based Access to Computers and Security Profiles

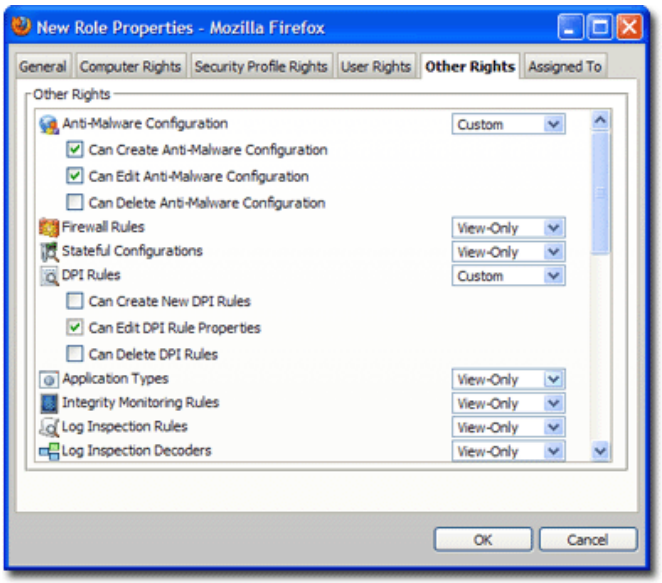
The access Roles have to computers and Security Profiles can be restricted to subsets of computers and Security Profiles. This can be controlled at a fairly granular level. For example, Users can be permitted to view all existing computers, but only permitted to modify those in a particular computer group.



Role-Based Editing Privileges

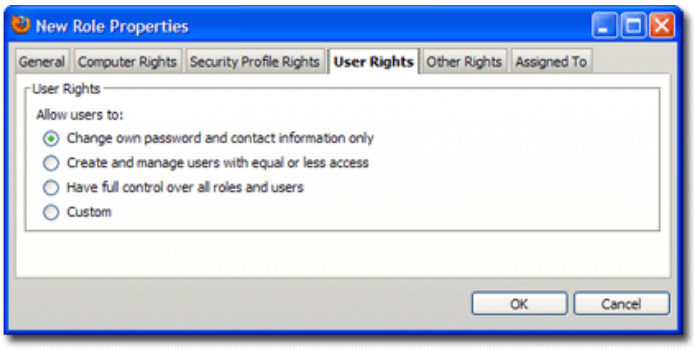
Within those access restrictions, Roles can have limitations placed on their editing privileges.

© Copyright 2011 Trend Micro Inc.
All rights reserved.



User rights

Users can be given delegated rights over other Users. That is, they can create and modify the properties only of Users with equal or less access than themselves.



Default Settings for Full Access, Auditor, and New Roles

The following table identifies the default rights settings for the **Full Access** Role and the **Auditor** Role. Also listed are the rights settings that are in place when creating a new Role by clicking **New** in the toolbar on the **Roles** screen.

RIGHTS	SETTINGS BY ROLE		
General	**Full Access Role**	**Auditor Role**	**New Role Defaults**
Access to DSM User Interface	Allowed	Allowed	Allowed
Access to Web Service API	Allowed	Allowed	Not allowed
Computer Rights	**Full Access Role**	**Auditor Role**	**New Role Defaults**
View	Allowed, All Computers	Allowed, All Computers	Allowed, All Computers
Edit	Allowed, All Computers	Not allowed, All Computers	Not allowed, All Computers

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Delete	Allowed, All Computers	Not allowed, All Computers	Not allowed, All Computers
Dismiss Alerts for	Allowed, All Computers	Not allowed, All Computers	Not allowed, All Computers
Tag Items for	Allowed, All Computers	Not allowed, All Computers	Not allowed, All Computers
View non-selected computers and data (e.g. events, reports)	Allowed	Allowed	Allowed, All Computers
View events and alerts not related to computers	Allowed	Allowed	Allowed, All Computers
Create new computers in selected groups	Allowed	Not allowed	Not allowed
Add or remove sub-groups in selected groups	Allowed	Not Allowed	Not allowed
Import computer files	Allowed	Not allowed	Not allowed
Add, remove, and synchronize Directories	Allowed	Not allowed	Not allowed
Add, remove, and synchronize VMware vCenters	Allowed	Not allowed	Not allowed
Security Profile Rights	**Full Access Role**	**Auditor Role**	**New Role Defaults**
View	Allowed, All Security Profiles	Allowed, All Security Profiles	Allowed, All Security Profiles
Edit	Allowed, All Security Profiles	Not allowed, All Security Profiles	Not allowed, All Security Profiles
Delete	Allowed, All Security Profiles	Not allowed, All Security Profiles	Not allowed, All Security Profiles
View non-selected security profiles	Allowed	Allowed	Allowed
Create new security profiles	Allowed	Not allowed	Not allowed
Import security profiles	Allowed	Not allowed	Not allowed
User Rights (See note on User rights below)	**Full Access Role**	**Auditor Role**	**New Role Defaults**
View Users	Allowed	Allowed	Not allowed
Create Users	Allowed	Not allowed	Not allowed
Edit User Properties	Allowed	Not allowed	Not allowed
Delete Users	Allowed	Not allowed	Not allowed
View Roles	Allowed	Allowed	Not allowed
Create Roles	Allowed	Not allowed	Not allowed
Edit Role Properties	Allowed	Not allowed	Not allowed
Delete Roles	Allowed	Not allowed	Not allowed

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Delegate Authority			
Other Rights	**Full Access Role**	**Auditor Role**	**New Role Defaults**
Alerts	Full (Can Dismiss Global Alerts)	View-Only	View-Only
Alert Configuration	Full (Can Edit Alert Configurations)	View-Only	View-Only
Anti-Malware Configuration	Full (Can Create, Edit, Delete Anti-Malware Configuration)	View-Only	View-Only
Quarantined File	Full (Can Delete, Download Quarantined File)	View-Only	View-Only
Firewall Rules	Full (Can Create, Edit, Delete Firewall Rules)	View-Only	View-Only
Stateful Configurations	Full (Can Create, Edit, Delete Stateful Configurations)	View-Only	View-Only
DPI Rules	Full (Can Create, Edit, Delete)	View-Only	View-Only
Application Types	Full (Can Create, Edit, Delete)	View-Only	View-Only
Integrity Monitoring Rules	Full (Can Create, Edit, Delete)	View-Only	View-Only
Log Inspection Rules	Full (Can Create, Edit, Delete)	View-Only	View-Only
Log Inspection Decoders	Full (Can Create, Edit, Delete)	View-Only	View-Only
Directory Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
Files Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
Files Extension Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
IP Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
MAC Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
Port Lists	Full (Can Create, Edit, Delete)	View-Only	View-Only
Contexts	Full (Can Create, Edit, Delete)	View-Only	View-Only
Schedules	Full (Can Create, Edit, Delete)	View-Only	View-Only
System Settings (Global)	Full (Can View, Edit System Settings (Global))	View-Only	Hide
System Information	Full (Can View System Information, Can Edit and Decommission Manager Nodes, Can Manage System Extensions)	View-Only	Hide
Diagnostics	Full (Can Create Diagnostic Packages)	View-Only	View-Only
Tagging (Advanced)	Full (Can Tag (Items not belonging to Computers), Can Delete Tags, Can Update Non-Owned Auto-Tag Rules, Can Run Non-Owned Auto-Tag Rules, Can Delete Non-Owned Auto-Tag Rules)	View-Only	View-Only
Tasks	Full (Can View, Add, Edit, Delete Tasks, Execute Tasks)	View-Only	Hide
Contacts	Full (Can View, Create, Edit, Delete Contacts)	View-Only	Hide
Licenses	Full (Can View, Change License)	View-Only	Hide
Updates	Full (Can Add, Edit, Delete	View-Only	Hide

© Copyright 2011 Trend Micro Inc.
All rights reserved.

	Software; Can View Update For Components; Can Download, Import, Apply Update Components; Can Delete Deep Security Rule Updates)		
Asset Values	Full (Can Create, Edit, Delete Asset Values)	View-Only	View-Only
Certificates	Full (Can Create, Delete SSL Certificates)	View-Only	View-Only

Note on User Rights

The **User Rights** area on the **User Rights** tab of the **Role Properties** screen has three general User rights options (**Change own password and contact information only**, **Create and manage users with equal or less access**, and **Have full control over all roles and users**) and a **Custom** option.

The custom settings corresponding to the **Change own password and contact information only** option are listed in the following table:

Custom settings corresponding to "Change own password and contact information only" option	
Users	
Can View Users	Not allowed
Can Create New Users	Not allowed
Can Edit User Properties (User can always edit select properties of own account)	Not allowed
Can Delete Users	Not allowed
Roles	
Can View Roles	Not allowed
Can Create New Roles	Not allowed
Can Edit Role Properties (Warning: conferring this right will let users with this role edit their own rights)	Not allowed
Can Delete Roles	Not allowed
Delegate Authority	
Can only manipulate users with equal or lesser rights	Not allowed

The custom settings corresponding to the **Create and manage users with equal or less access** option are listed in the following table:

Custom settings corresponding to "Create and manage users with equal or less access" option	
Users	
Can View Users	Allowed
Can Create New Users	Allowed

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Can Edit User Properties (User can always edit select properties of own account)	Allowed
Can Delete Users	Allowed
Roles	
Can View Roles	Not allowed
Can Create New Roles	Not allowed
Can Edit Role Properties (Warning: conferring this right will let users with this role edit their own rights)	Not allowed
Can Delete Roles	Not allowed
Delegate Authority	
Can only manipulate users with equal or lesser rights	Allowed

The custom settings corresponding to the **Have full control over all roles and users** option are listed in the following table:

Custom settings corresponding to "Have full control over all roles and users" option	
Users	
Can View Users	Allowed
Can Create New Users	Allowed
Can Edit User Properties (User can always edit select properties of own account)	Allowed
Can Delete Users	Allowed
Roles	
Can View Roles	Allowed
Can Create New Roles	Allowed
Can Edit Role Properties (Warning: conferring this right will let users with this role edit their own rights)	Allowed
Can Delete Roles	Allowed
Delegate Authority	
Can only manipulate users with equal or lesser rights	N/A

© Copyright 2011 Trend Micro Inc.
All rights reserved.

System Events

The following table lists the System Events that can be recorded by Deep Security and their default settings. (Notifications cannot be sent for Events that are not recorded.)

Number	Severity	Event	Record	Notify	Notes
0	Error	Unknown Error	On	On	
100	Info	Deep Security Manager Started	On	On	
101	Info	License Changed	On	On	
102	Info	Trend Micro Deep Security Customer Account Changed	On	On	
103	Warning	Check For Updates Failed	On	On	
104	Warning	Automatic Software Download Failed	On	On	
105	Warning	Scheduled Deep Security Rule Update Download and Apply Failed	On	On	
106	Info	Scheduled Deep Security Rule Update Downloaded and Applied	On	On	
107	Info	Deep Security Rule Update Downloaded and Applied	On	On	
108	Info	Script Executed	On	On	
109	Error	Script Execution Failed	On	On	
110	Info	System Events Exported	On	On	
111	Info	Firewall Events Exported	On	On	
112	Info	DPI Events Exported	On	On	
113	Warning	Scheduled Deep Security Rule Update Download Failed	On	On	
114	Info	Scheduled Deep Security Rule Update Downloaded	On	On	
115	Info	Deep Security Rule Update Downloaded	On	On	
116	Info	Deep Security Rule Update Applied	On	On	
117	Info	Deep Security Manager Shutdown	On	On	
118	Warning	Deep Security Manager Offline	On	On	
119	Info	Deep Security Manager Back Online	On	On	
120	Error	Heartbeat Server Failed	On	On	
121	Error	Scheduler Failed	On	On	
122	Error	Manager Message Thread Failed	On	On	
123	Info	Deep Security Manager Forced Shutdown	On	On	
124	Info	Deep Security Rule Update Deleted	On	On	
130	Info	Credentials Generated	On	On	
131	Warning	Credential Generation Failed	On	On	
140	Info	Discover Computers	On	On	
141	Warning	Discover Computers Failed	On	On	
142	Info	Discover Computers Requested	On	On	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

143	Info	Discover Computers Cancelled	On	On	
150	Info	System Settings Saved	On (cannot be turned off)	On	
151	Info	Software Added	On	On	
152	Info	Software Deleted	On	On	
153	Info	Software Updated	On	On	
154	Info	Software Exported	On	On	
155	Info	Software Platforms Changed	On	On	
160	Info	Authentication Failed	On	On	
161	Info	Deep Security Rule Update Exported	On	On	
162	Info	Log Inspection Events Exported	On	On	
163	Info	Anti-Malware Event Exported	On	On	
164	Info	Anti-Malware Component Update Success	On	On	
165	Error	Anti-Malware Component Update Failed	On	On	
166	Info	Check for New Software Success	On	On	
167	Error	Check for New Software Failed	On	On	
168	Info	Manual Update Component Success	On	On	
169	Error	Manual Update Component Failed	On	On	
170	Error	Manager Available Disk Space Too Low	On	On	
180	Info	Alert Type Updated	On	On	
190	Info	Alert Started	On	On	
191	Info	Alert Changed	On	On	
192	Info	Alert Ended	On	On	
197	Info	Alert Emails Sent	On	On	
198	Warning	Alert Emails Failed	On	On	
199	Error	Alert Processing Failed	On	On	
250	Info	Computer Created	On	On	
251	Info	Computer Deleted	On	On	
252	Info	Computer Updated	On	On	
253	Info	Security Profile Assigned to Computer	On	On	
254	Info	Computer Moved	On	On	
255	Info	Activation Requested	On	On	
256	Info	Update Now Requested	On	On	
257	Info	Locked	On	On	
258	Info	Unlocked	On	On	
259	Info	Deactivation Requested	On	On	
260	Info	Scan for Open Ports	On	On	
261	Warning	Scan for Open Ports Failed	On	On	
262	Info	Scan for Open Ports Requested	On	On	
263	Info	Scan for Open Ports Cancelled	On	On	
264	Info	Agent Software Upgrade Requested	On	On	
265	Info	Agent Software Upgrade Cancelled	On	On	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

266	Info	Warnings/Errors Cleared	On	On	
267	Info	Check Status Requested	On	On	
268	Info	Get Events Now Requested	On	On	
270	Error	Computer Creation Failed	On	On	
273	Info	Anti-Malware Component Update Requested	On	On	
275	Warning	Duplicate Computer	On	On	
276	Info	Components Updated	On	On	
280	Info	Computers Exported	On	On	
281	Info	Computers Imported	On	On	
286	Info	Computer Log Exported	On	On	
290	Info	Group Added	On	On	
291	Info	Group Removed	On	On	
292	Info	Group Updated	On	On	
293	Info	Interface Renamed	On	On	
294	Info	Computer Bridge Renamed	On	On	
295	Info	Interface Deleted	On	On	
296	Info	Interface IP Deleted	On	On	
297	Info	Scan for Recommendations Requested	On	On	
298	Info	Recommendations Cleared	On	On	
299	Info	Asset Value Assigned to Computer	On	On	
300	Info	Scan for Recommendations	On	On	
301	Info	Agent Software Deployment Requested	On	On	
302	Info	Agent Software Removal Requested	On	On	
303	Info	Computer Renamed	On	On	
305	Info	Scan for Integrity Changes Requested	On	On	
306	Info	Rebuild Baseline Requested	On	On	
307	Info	Cancel Update Requested	On	On	
308	Info	Integrity Monitoring Rule Compile Issue	On	On	
309	Info	Integrity Monitoring Rule Compile Issue Resolved	On	On	
310	Info	Directory Added	On	On	
311	Info	Directory Removed	On	On	
312	Info	Directory Updated	On	On	
320	Info	Directory Synchronization	On	On	
321	Info	Directory Synchronization Finished	On	On	
322	Error	Directory Synchronization Failed	On	On	
323	Info	Directory Synchronization Requested	On	On	
324	Info	Directory Synchronization Cancelled	On	On	
325	Info	User Synchronization	On	On	
326	Info	User Synchronization Finished	On	On	
327	Error	User Synchronization Failed	On	On	
328	Info	User Synchronization Requested	On	On	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

329	Info	User Synchronization Cancelled	On	On	
330	Info	SSL Configuration Created	On	On	
331	Info	SSL Configuration Deleted	On	On	
332	Info	SSL Configuration Updated	On	On	
350	Info	Security Profile Created	On	On	
351	Info	Security Profile Deleted	On	On	
352	Info	Security Profile Updated	On	On	
353	Info	Security Profiles Exported	On	On	
354	Info	Security Profiles Imported	On	On	
360	Info	VMware vCenter Added	On	On	
361	Info	VMware vCenter Removed	On	On	
362	Info	VMware vCenter Updated	On	On	
363	Info	VMware vCenter Synchronization	On	On	
364	Info	VMware vCenter Synchronization Finished	On	On	
365	Error	VMware vCenter Synchronization Failed	On	On	
366	Info	VMware vCenter Synchronization Requested	On	On	
367	Info	VMware vCenter Synchronization Cancelled	On	On	
368	Warning	Interfaces Out of Sync	On	On	
369	Info	Interfaces in Sync	On	On	
370	Info	ESX Server Prepared	On	On	
371	Info	ESX Server Restored	On	On	
372	Info	Filter Driver Upgraded	On	On	
373	Info	Virtual Appliance Deployed	On	On	
374	Info	Virtual Appliance Upgraded	On	On	
375	Warning	Virtual Appliance Upgrade Failed	On	On	
376	Warning	Virtual Machine moved to unprotected ESX	On	On	
377	Info	Virtual Machine moved to protected ESX	On	On	
378	Warning	Virtual Machine unprotected during move to another ESX	On	On	
379	Info	Virtual Machine unprotected during move to another ESX Resolved	On	On	
380	Error	Filter Driver Offline	On	On	
381	Info	Filter Driver Back Online	On	On	
382	Info	Filter Driver Upgrade Requested	On	On	
383	Info	Appliance Upgrade Requested	On	On	
384	Warning	Prepare ESX Failed	On	On	
385	Warning	Filter Driver Upgrade Failed	On	On	
386	Warning	Restore ESX Failed	On	On	
387	Error	Connection to Filter Driver Failure	On	On	
388	Info	Connection to Filter Driver Success	On	On	
389	Error	Multiple Activated Appliances Detected	On	On	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

390	Info	Multiple Activated Appliances Detected Resolved	On	On	
391	Error	Network Settings Out of Sync With vCenter Global Settings	On	On	
392	Info	Network Settings in Sync With vCenter Global Settings	On	On	
393	Error	Anti-Malware Driver Offline	On	On	
394	Info	Anti-Malware Driver Back Online	On	On	
395	Error	Virtual Appliance is incompatible with Filter Driver	On	On	
396	Info	Virtual Appliance is incompatible with Filter Driver resolved	On	On	
410	Info	Firewall Rule Created	On	On	
411	Info	Firewall Rule Deleted	On	On	
412	Info	Firewall Rule Updated	On	On	
413	Info	Firewall Rule Exported	On	On	
414	Info	Firewall Rule Imported	On	On	
420	Info	Stateful Configuration Created	On	On	
421	Info	Stateful Configuration Deleted	On	On	
422	Info	Stateful Configuration Updated	On	On	
423	Info	Stateful Configuration Exported	On	On	
424	Info	Stateful Configuration Imported	On	On	
460	Info	Application Type Created	On	On	
461	Info	Application Type Deleted	On	On	
462	Info	Application Type Updated	On	On	
463	Info	Application Type Exported	On	On	
464	Info	Application Type Imported	On	On	
470	Info	DPI Rule Created	On	On	
471	Info	DPI Rule Deleted	On	On	
472	Info	DPI Rule Updated	On	On	
473	Info	DPI Rule Exported	On	On	
474	Info	DPI Rule Imported	On	On	
480	Info	Integrity Monitoring Rule Created	On	On	
481	Info	Integrity Monitoring Rule Deleted	On	On	
482	Info	Integrity Monitoring Rule Updated	On	On	
483	Info	Integrity Monitoring Rule Exported	On	On	
484	Info	Integrity Monitoring Rule Imported	On	On	
490	Info	Log Inspection Rule Created	On	On	
491	Info	Log Inspection Rule Deleted	On	On	
492	Info	Log Inspection Rule Updated	On	On	
493	Info	Log Inspection Rule Exported	On	On	
494	Info	Log Inspection Rule Imported	On	On	
495	Info	Log Inspection Decoder Created	On	On	
496	Info	Log Inspection Decoder Deleted	On	On	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

497	Info	Log Inspection Decoder Updated	On	On	
498	Info	Log Inspection Decoder Exported	On	On	
499	Info	Log Inspection Decoder Imported	On	On	
505	Info	Context Created	On	On	
506	Info	Context Deleted	On	On	
507	Info	Context Updated	On	On	
508	Info	Context Exported	On	On	
509	Info	Context Imported	On	On	
510	Info	IP List Created	On	On	
511	Info	IP List Deleted	On	On	
512	Info	IP List Updated	On	On	
513	Info	IP List Exported	On	On	
514	Info	IP List Imported	On	On	
520	Info	Port List Created	On	On	
521	Info	Port List Deleted	On	On	
522	Info	Port List Updated	On	On	
523	Info	Port List Exported	On	On	
524	Info	Port List Imported	On	On	
530	Info	MAC List Created	On	On	
531	Info	MAC List Deleted	On	On	
532	Info	MAC List Updated	On	On	
533	Info	MAC List Exported	On	On	
534	Info	MAC List Imported	On	On	
550	Info	Schedule Created	On	On	
551	Info	Schedule Deleted	On	On	
552	Info	Schedule Updated	On	On	
553	Info	Schedule Exported	On	On	
554	Info	Schedule Imported	On	On	
560	Info	Scheduled Task Created	On	On	
561	Info	Scheduled Task Deleted	On	On	
562	Info	Scheduled Task Updated	On	On	
563	Info	Scheduled Task Manually Executed	On	On	
564	Info	Scheduled Task Started	On	On	
565	Info	Backup Finished	On	On	
566	Error	Backup Failed	On	On	
567	Info	Sending Outstanding Alert Summary	On	On	
568	Warning	Failed To Send Outstanding Alert Summary	On	On	
569	Warning	Email Failed	On	On	
570	Info	Sending Report	On	On	
571	Warning	Failed To Send Report	On	On	
572	Error	Invalid Report Jar	On	On	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

573	Info	Asset Value Created	On	On	
574	Info	Asset Value Deleted	On	On	
575	Info	Asset Value Updated	On	On	
576	Error	Report Uninstall Failed	On	On	
577	Error	Report Uninstalled	On	On	
580	Warning	Application Type Port List Misconfiguration	On	On	
581	Warning	Application Type Port List Misconfiguration Resolved	On	On	
582	Warning	DPI Rules Require Configuration	On	On	
583	Info	DPI Rules Require Configuration Resolved	On	On	
584	Warning	Integrity Monitoring Rules Require Configuration	On	On	
585	Info	Integrity Monitoring Rules Require Configuration Resolved	On	On	
586	Warning	Log Inspection Rules Require Configuration	On	On	
587	Info	Log Inspection Rules Require Configuration Resolved	On	On	
588	Warning	Log Inspection Rules Require Log Files	On	On	
589	Info	Log Inspection Rules Require Log Files Resolved	On	On	
590	Warning	Scheduled Task Unknown Type	On	On	
600	Info	User Signed In	On	On	
601	Info	User Signed Out	On	On	
602	Info	User Timed Out	On	On	
603	Info	User Locked Out	On	On	
604	Info	User Unlocked	On	On	
608	Error	User Session Validation Failed	On	On	
609	Error	User Made Invalid Request	On	On	
610	Info	User Session Validated	Off	Off	
611	Info	User Viewed Firewall Event	Off	Off	
613	Info	User Viewed DPI Event	Off	Off	
615	Info	User Viewed System Event	Off	Off	
616	Info	User Viewed Integrity Monitoring Event	Off	Off	
617	Info	User Viewed Log Inspection Event	Off	Off	
618	Info	User Viewed Quarantined File Detail	Off	Off	
619	Info	User Viewed Anti-Malware Event	Off	Off	
650	Info	User Created	On	On	
651	Info	User Deleted	On	On	
652	Info	User Updated	On	On	
653	Info	User Password Set	On	On	
660	Info	Role Created	On	On	
661	Info	Role Deleted	On	On	
662	Info	Role Updated	On	On	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

663	Info	Roles Imported	On	On	
664	Info	Roles Exported	On	On	
670	Info	Contact Created	On	On	
671	Info	Contact Deleted	On	On	
672	Info	Contact Updated	On	On	
700	Info	Agent Software Installed	On	On	
701	Error	Agent Software Installation Failed	On	On	
702	Info	Credentials Generated	On	On	
703	Error	Credential Generation Failed	On	On	
704	Info	Activated	On	On	
705	Error	Activation Failed	On	On	
706	Info	Agent Software Upgraded	On	On	
707	Warning	Agent Software Upgrade Failed	On	On	
708	Info	Deactivated	On	On	
709	Error	Deactivation Failed	On	On	
710	Info	Events Retrieved	On	On	
711	Info	Agent Software Deployed	On	On	
712	Error	Agent Software Deployment Failed	On	On	
713	Info	Agent Software Removed	On	On	
714	Error	Agent Software Removal Failed	On	On	
715	Info	Agent/Appliance Version Changed	On	On	
720	Info	Updated	On	On	Agent/Appliance updated.
721	Error	Update Failed	On	On	
722	Warning	Get Interfaces Failed	On	On	s
723	Info	Get Interfaces Failure Resolved	On	On	
724	Warning	Insufficient Disk Space	On	On	
725	Warning	Events Suppressed	On	On	
726	Warning	Get Agent/Appliance Events Failed	On	On	
727	Info	Get Agent/Appliance Events Failure Resolved	On	On	
728	Error	Get Events Failed	On	On	
729	Info	Get Events Failure Resolved	On	On	
730	Error	Offline	On	On	
731	Info	Back Online	On	On	
732	Error	Firewall Rule Engine Offline	On	On	
733	Info	Firewall Rule Engine Back Online	On	On	
734	Warning	Computer Clock Change	On	On	
735	Warning	Misconfiguration Detected	On	On	
736	Info	Check Status Failure Resolved	On	On	
737	Error	Check Status Failed	On	On	
738	Error	DPI Rule Engine Offline	On	On	
739	Info	DPI Rule Engine Back Online	On	On	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

740	Error	Agent/Appliance Error	On	On	
741	Warning	Abnormal Restart Detected	On	On	
742	Warning	Communications Problem	On	On	
743	Info	Communications Problem Resolved	On	On	
745	Warning	Events Truncated	On	On	
748	Error	Log Inspection Engine Offline	On	On	
749	Info	Log Inspection Engine Back Online	On	On	
750	Warning	Last Automatic Retry	On	On	
755	Info	Deep Security Manager Version Compatibility Resolved	On	On	
756	Warning	Deep Security Manager Upgrade Recommended (Incompatible Security Component(s))	On	On	
760	Info	Agent/Appliance Version Compatibility Resolved	On	On	
761	Warning	Agent/Appliance Upgrade Recommended	On	On	
762	Warning	Agent/Appliance Upgrade Required	On	On	
763	Warning	Incompatible Agent/Appliance Version	On	On	
764	Warning	Agent/Appliance Upgrade Recommended (Incompatible Security Component(s))	On	On	
765	Warning	Computer Reboot Required	On	On	
766	Warning	Network Engine Mode Configuration Incompatibility	On	On	
767	Warning	Network Engine Mode Version Incompatibility	On	On	
768	Warning	Network Engine Mode Incompatibility Resolved	On	On	
770	Warning	Agent/Appliance Heartbeat Rejected	On	On	
771	Warning	Contact by Unrecognized Client	On	On	
780	Info	Scan for Recommendations Failure Resolved	On	On	
781	Warning	Scan for Recommendations Failure	On	On	
782	Info	Integrity Monitoring Failure Resolved	On	On	
783	Warning	Integrity Monitoring Failure	On	On	
784	Info	Component Update Success	On	On	
785	Warning	Component Update Failure	On	On	
790	Info	Agent Initiated Activation Requested	On	On	
791	Warning	Agent Initiated Activation Failure	On	On	
792	Info	Anti-Malware Manual Scan Failure Resolved	On	On	
793	Warning	Anti-Malware Manual Scan Failure	On	On	
794	Info	Anti-Malware Scheduled Scan Failure Resolved	On	On	
795	Warning	Anti-Malware Scheduled Scan Failure	On	On	
796	Info	Anti-Malware Scheduled Scan Task Has Been Missed	On	On	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

797	Info	Anti-Malware Cancel Scan Failure Resolved	On	On	
798	Warning	Anti-Malware Cancel Scan Failure	On	On	
799	Warning	Anti-Malware Scan Stalled	On	On	
800	Info	Alert Dismissed	On	On	
801	Info	Error Dismissed	On	On	
850	Warning	Reconnaissance Detected: Computer OS Fingerprint Probe	On	On	
851	Warning	Reconnaissance Detected: Network or Port Scan	On	On	
852	Warning	Reconnaissance Detected: TCP Null Scan	On	On	
853	Warning	Reconnaissance Detected: TCP SYNFIN Scan	On	On	
854	Warning	Reconnaissance Detected: TCP Xmas Scan	On	On	
900	Info	Deep Security Manager Audit Started	On	On	
901	Info	Deep Security Manager Audit Shutdown	On	On	
902	Info	Deep Security Manager Installed	On	On	
903	Warning	License Related Configuration Change	On	On	
910	Info	Diagnostic Package Generated	On	On	
911	Info	Diagnostic Package Exported	On	On	
912	Info	Diagnostic Package Uploaded	On	On	
913	Error	Automatic Diagnostic Package Error	On	On	
914	Info	Quarantined File Deletion Succeeded	On	On	
915	Info	Quarantined File Deletion Failed	On	On	
916	Info	Quarantined File Download Succeeded	On	On	
917	Info	Quarantined File Download Failed	On	On	
918	Info	Quarantined File Administration Utility Download Succeeded	On	On	
919	Info	Quarantined File Not Found	On	On	
920	Info	Usage Information Generated	On	On	
921	Info	Usage Information Package Exported	On	On	
922	Info	Usage Information Package Uploaded	On	On	
923	Error	Usage Information Package Error	On	On	
924	Error	Anti-Malware Quarantine Failed (VM limit exceeded)	On	On	
925	Error	Anti-Malware Quarantine Failed (Appliance limit exceeded)	On	On	
926	Error	Smart Scan Server Disconnected	On	On	
927	Info	Smart Scan Server Connected	On	On	
930	Info	Certificate Accepted	On	On	
931	Info	Certificate Deleted	On	On	
940	Info	Auto-Tag Rule Created	On	On	
941	Info	Auto-Tag Rule Deleted	On	On	
942	Info	Auto-Tag Rule Updated	On	On	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

943	Info	Tag Deleted	On	On	
970	Info	Command Line Utility Started	On	On	
978	Info	Command Line Utility Failed	On	On	
979	Info	Command Line Utility Shutdown	On	On	
980	Info	System Information Exported	On	On	
990	Info	Manager Node Added	On	On	
991	Info	Manager Node Decommissioned	On	On	
992	Info	Manager Node Updated	On	On	
997	Error	Tagging Error	On	On	
998	Error	System Event Notification Error	On	On	
999	Error	Internal Software Error	On	On	
1101	Error	Plug-in Installation Failed	On	On	
1102	Info	Plug-in Installed	On	On	
1103	Error	Plug-in Upgrade Failed	On	On	
1104	Info	Plug-in Upgraded	On	On	
1105	Error	Plug-in Start Failed	On	On	
1106	Error	Plug-in Uninstall Failed	On	On	
1107	Info	Plug-in Uninstalled	On	On	
1500	Info	Anti-Malware Configuration Created	On	On	
1501	Info	Anti-Malware Configuration Deleted	On	On	
1502	Info	Anti-Malware Configuration Updated	On	On	
1503	Info	Anti-Malware Configuration Exported	On	On	
1504	Info	Anti-Malware Configuration Imported	On	On	
1505	Info	Directory List Created	On	On	
1506	Info	Directory List Deleted	On	On	
1507	Info	Directory List Updated	On	On	
1508	Info	Directory List Imported	On	On	
1509	Info	Directory List Exported	On	On	
1510	Info	File Extension List Created	On	On	
1511	Info	File Extension List Deleted	On	On	
1512	Info	File Extension List Updated	On	On	
1513	Info	File Extension List Imported	On	On	
1514	Info	File Extension List Exported	On	On	
1515	Info	File List Created	On	On	
1516	Info	File List Deleted	On	On	
1517	Info	File List Updated	On	On	
1518	Info	File List Imported	On	On	
1519	Info	File List Exported	On	On	
1520	Info	Anti-Malware Manual Scan Pending For Start	On	On	
1521	Info	Anti-Malware Manual Scan Started	On	On	
1522	Info	Anti-Malware Manual Scan Completed	On	On	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

1523	Info	Anti-Malware Scheduled Scan Started	On	On	
1524	Info	Anti-Malware Scheduled Scan Completed	On	On	
1525	Info	Anti-Malware Manual Scan Cancellation In Progress	On	On	
1526	Info	Anti-Malware Manual Scan Cancellation Completed	On	On	
1527	Info	Anti-Malware Scheduled Scan Cancellation In Progress	On	On	
1528	Info	Anti-Malware Scheduled Scan Cancellation Completed	On	On	
1529	Info	Anti-Malware Manual Scan Paused	On	On	
1530	Info	Anti-Malware Manual Scan Resumed	On	On	
1531	Info	Anti-Malware Scheduled Scan Paused	On	On	
1532	Info	Anti-Malware Scheduled Scan Resumed	On	On	

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Teamed NICs

Installing the Windows and Solaris Agents in a Teamed NICs Environment

"Teamed NICs" describes using multiple ethernet adapters in parallel to increase data transfer speed or to provide redundancy. The following information provides guidance for configuring teamed NICs installations in Windows and Solaris so that they are compatible with the Deep Security Agent. If you encounter difficulties, please contact your support provider.

Windows

Windows NIC teaming software creates a new virtual master interface which adopts the MAC address of the first slave interface. By default, the Windows Agent will bind to all virtual and physical interfaces during installation. As a result, in a teamed NIC environment the Agent will bind to the physical interfaces as well as the virtual interface created by the teaming software. The Agent cannot function properly with multiple interfaces having the same MAC address. To function properly, the Agent must be bound only to the virtual interface created by the teaming software.

Using the Agent in a teamed NICs environment on Windows 2003 requires SP 2 or later, or the installation of the following patch: http://support.microsoft.com/kb/912222/article

Using the Agent in a teamed NICs environment on Windows 2000 is not supported.

The Agent's network driver is bound to the network interfaces only at install or upgrade time. After installation, it is not possible for the bindings to be automatically adjusted when you add or remove network interfaces to or from a Teamed NIC. Doing so can lead to network connectivity problems, or to the host system not being properly protected. After adding or removing a network interface in a teamed environment where the Agent's network driver is installed, you should verify that the driver is only bound to the virtual interface and not bound to any physical adapters.

Solaris

IPMP failover (active-standby) mode in Solaris allows two NICs to have the same hardware (MAC) address. Since the Deep Security Agent identifies adapters by their MAC address, such duplication prevents the Agent from functioning properly.

The solution is to manually assign unique MAC addresses to each adapter.

Sample ifconfig output:

```
# ifconfig -a
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
inet 10.20.30.40 netmask 0
ether 8:0:20:f7:c3:f

hme1: flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 8
inet 0.0.0.0 netmask 0
ether 8:0:20:f7:c3:f
```

© Copyright 2011 Trend Micro Inc.
All rights reserved.

The "ether" line displays the adapter's MAC address. If any interfaces are showing identical MAC addresses and are connected to the same subnet, new unique MAC addresses must be set manually using the following ifconfig command:

```
# ifconfig <interface> ether <new MAC address>
```

Although the chance of a MAC address conflict is extremely small, you should verify that there isn't one by using the snoop command to search for the chosen MAC address. Then use the ping command to test connection to the broadcast address of the subnet.

On Solaris systems with multiple interfaces on the same subnet, the operating system may route packets through any of the interfaces. Because of this, any Stateful Configuration options or DPI Rules should be applied to all interfaces equally.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Virtual Appliance

The Deep Security Virtual Appliance provides Anti-Malware, Firewall, Intrusion Detection/Prevention, Application Control, and Web Application Protection Services to virtual machines in a VMware vSphere environment without requiring the presence of an in-guest Deep Security Agent. The Virtual Appliance uses VMware's VMsafe-NET API to intercept network traffic at the hypervisor. Virtual machines are managed as though they had an Agent installed.

The Virtual Appliance provides some distinct security advantages over scenarios with an in-guest Agent:

- The Appliance is isolated from the guest. The guest can operate with only the minimum required software being installed.
- Short-lived and reverted machines for which administrator time may not have been allocated for installing security software can easily and quickly be protected.
- Virtual machines and other Appliances whose operating systems are not directly accessible can be protected, even those machines being managed by other administrators.
- The Deep Security Virtual Appliance is easier to deploy. There is no need to remotely install Agent software on the virtual machine. Even connectivity to the virtual machine is not required.

As well, using the Virtual Appliance allows you to protect guests running operating systems not directly supported by Deep Security Agents.

Using the Virtual Appliance to protect virtual machines doesn't preclude the use of Deep Security Agents on those virtual machines. This Coordinated Approach provides the following benefits:

- Allows you to implement the additional Integrity Monitoring and Log Inspection modules on the virtual machine.
- Recommendation Scans can be run on the virtual machines.
- Provides mobility to the virtual machines. They can be moved between data centers or cloud providers and the protection moves with them.
- Performance improvement. While the Deep Security Agent is active on the virtual machine, the Virtual Appliance automatically passes traffic through to the Agent.

VMware Environment for Anti-Malware Protection

VMware

- **Operating System:** VMware vCenter 4.1.0 and ESXi 4.1.0
- **Software:** VMware vShield Manager, and VMware vShield Endpoint 1.0 (including VMware Endpoint Thin Agents for each virtual machine.)

The VMware vCenter manages the ESXi servers which host the guest VMs that are to be protected. The VMware vShield Manager manages VMware vShield Endpoint which in turn communicates with the VMware Thin Agents. The last two components provide the API which Deep Security uses to provide Anti-Malware protection.

Deep Security

- **Software:** Deep Security Manager 7.5, Deep Security Virtual Appliance 7.5, and Deep Security Filter Driver 7.5.

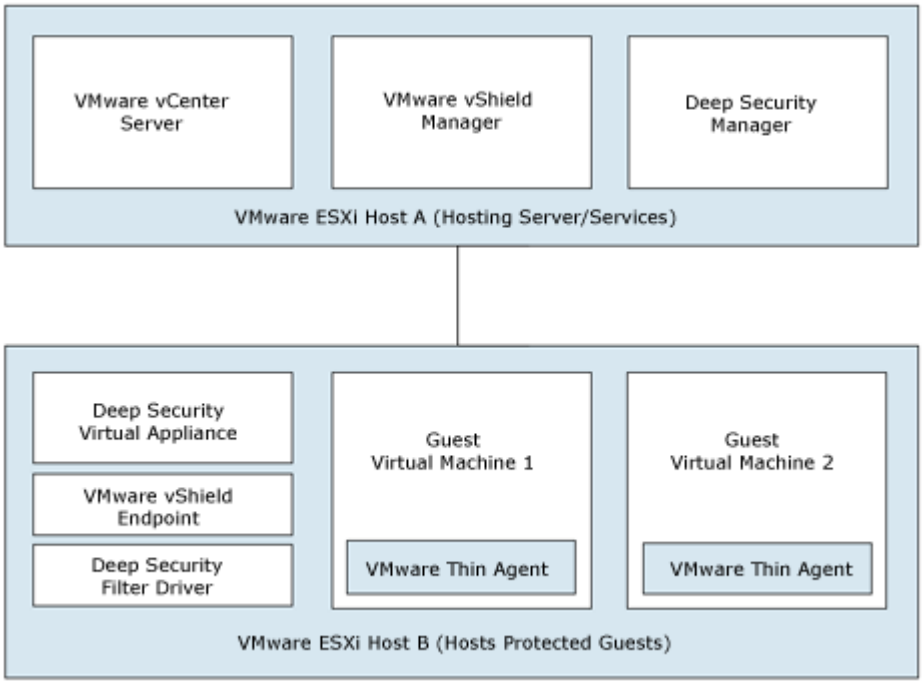
The Deep Security Manager coordinate the Anti-Malware protection being provided to each guest virtual machine. This is done through the Deep Security Virtual Appliance which uses the VMware Endpoint API to

© Copyright 2011 Trend Micro Inc.
All rights reserved.

apply the protection to the virtual machines. The Deep Security Filter driver controls network traffic in and out of the guest virtual machines.

The vShield Manager and the Deep Security Manager must not be installed on the same ESXi server that is hosting the guest virtual machines being protected.

The following diagram illustrates a typical environment:



For instructions on implementing Deep Security Anti-Malware protection in a VMware environment, consult your Trend Micro Deep Security 7.5 Installation Guide.

Implementing VM Protection with the Deep Security Virtual Appliance

Implementing VM Protection with the Deep Security Virtual Appliance involves:

1. Adding the VMware vCenter to the list of managed computers
2. Preparing the ESX Server for the Virtual Appliance deployment

Note that ESX Servers cannot be added to the list of managed computers without first adding the supporting VMware vCenter.

3. Deploying the Virtual Appliance to the ESX Server
4. Manually assigning an IP address to the Virtual Appliance (*only required if the Virtual Appliance does not have access to a DHCP server*)
5. Activating the Virtual Appliance
6. Enabling Virtual Appliance protection on guest virtual machines
7. Optionally, installing Deep Security Agents on the virtual machines to implement the Coordinated Approach for VM protection

© Copyright 2011 Trend Micro Inc.
All rights reserved.

To add a VMware vCenter to the list of managed computers:

1. Right-click on **Computers** in the navigation pane and select **Add VMware vCenter...** to start the **Add VMware vCenter** wizard.
2. Provide the server address (IP or hostname) and port, a name and description, and the username and password for the ESX Server. Click **Next**.
3. The **Add VMware vCenter** wizard will display the details of the vCenter being added.
4. Click **Finish**.

Real-time synchronization will be maintained with this VMware vCenter to keep the information displayed in the Deep Security Manager up-to-date (number of VMs, their status, etc.).

The VMware vCenter is now displayed among your other computers on the **Computers** screen.

To prepare the ESX Server for the Virtual Appliance deployment:

Note that Windows XP (64-bit) and Windows 2003 (64-bit) must both be patched to at least SP2 to allow Coordinated Approach protection (a virtual machine being protected by both an Agent and a Virtual Appliance.)

1. Under **Computers** in the Deep Security Manager navigation pane, click on the newly added vCenter to display the various vCenter components on the **Computers** screen.
2. Find the ESX Server on the **Computers** screen (its **Status** column should read "Unprepared"), right-click on it, and select **Actions > Prepare ESX Server** to display the **Prepare ESX Server** wizard. Click **Next**.
3. The ESX Server must be put into maintenance mode before the first of two Virtual Appliance components (the Filter Driver) can be installed. Select **Yes** to allow the Deep Security Manager to manage this process automatically. Click **Next**.
4. On the **DVFilter Configuration** screen, accept the default values and click **Next**.
5. The ESX Server will now be placed in maintenance mode, the Filter Driver will be installed, and the ESX Server will be restarted. When the wizard indicates that the process is complete, click **Close**.

You can monitor this process in the VMware vSphere Client management console.

The Filter Driver is now installed on the ESX Server.

To deploy the Virtual Appliance to the ESX Server:

1. Right-click on the ESX Server on the **Computers** screen (the **Status** column should now read "Prepared"), and select **Actions > Deploy Appliance** to display the **Deep Security Virtual Appliance** wizard. Click **next**.
2. Give the Virtual Appliance a name and click **Finish**.
3. The Virtual Appliance will now be deployed on the ESX Server. (Once again, this procedure can be monitored in the VMware vSphere Client management console.) When the Virtual Appliance deployment is complete, click **Close**.

The Virtual Appliance is now displayed along with the other computers in the vCenter group on the **Computers** screen.

To manually assign an IP address to the Virtual Appliance (*only required if the Virtual Appliance doesn't have access to a DHCP server*):

1. Log in to the vSphere client
2. Select the Virtual Appliance
3. View the console
4. Press F2
5. Log in using username/password: dsva/dsva
6. Select **Configure Management Network**
7. Specify a hostname and /or an IP address, subnet mask, default gateway, and DNS
8. Press **Enter** to save changes

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Although the changes will take effect immediately, the Virtual Appliance must be restarted for the new IP address to be displayed.

To activate the Virtual Appliance on the ESX Server:

1. Right-click on the Virtual Appliance in the computer list and select **Actions > Activate Appliance** to display the **Activate Deep Security Appliance** wizard. Click **Next**.
2. **Appliance VNIC IP:** This must be an otherwise unused IP address. The wizard will provide a default. **Security Profile:** Select **None**. Click **Next**.
3. When the Virtual Appliance has been successfully activated, click **Close**.

The **Status** of the Virtual Appliance will now read "Managed (Online)".

To enable Virtual Appliance protection on guest virtual machines:

1. Right-click on a virtual machine in the computer list and select **Actions > Activate**.
2. The **Status** column for the virtual machine will change to "Managed (Online)".

The virtual machine is now protected by the Virtual Appliance even though no in-guest Agent is installed on the virtual machine. Firewall Rules and DPI Rules (and Security Profiles) can be assigned to this virtual machine like any other computer being managed by Deep Security Manager.

Once the Virtual Appliance is installed, any virtual machines that are added to the ESX server afterwards can be automatically activated and a Security Profile can be automatically applied. To enable these options, go to **System > System Settings > Computers** and set the options in the **vCenter Options** area. (These options are off by default.)

The Virtual Appliance requires that all VMs that are to be protected have been assigned unique UUIDs by the vCenter. A situation with duplicate UUIDs can occur if you copy a VM. After copying a VM, you are asked by vCenter whether the new VM is a copy or whether it was moved. If you select the **I copied it** option, vCenter will assign it a new UUID. However, if you select the **I moved it** option (when in fact it was copied), vCenter will not assign it a new UUID. You will then have two VMs with the same UUID which will cause problems for the Virtual Appliance. If the Virtual Appliance is instructed to protect multiple VMs with the same UUID, an alert will be raised and the operation will fail.

To implement coordinated protection by installing an Agent on a virtual machine:

To install a Deep Security Agent on a virtual machine, follow the same procedures as for any "real" computer. A virtual machine being protected by both a Virtual Appliance and an Agent is referred to as "coordinated protection". The Virtual Appliance and the Agent are in constant communication. As long as the Virtual Appliance detects the presence of an Agent on the virtual machine, it will pass all traffic to the Agent and let the Agent apply the security rules to the traffic. If the Agent fails or is stopped, the Virtual Appliance will take over the job of applying security rules to traffic.

When a Security Profile is applied to an Agent on a VM that is also protected by a Virtual Appliance, then a copy of that profile also goes to the Virtual Appliance. When the Agent is running on a VM, the Virtual Appliance is actually sitting idle. If the communication between the Virtual Appliance and the Agent is interrupted (by the Agent going offline for some reason), then the Appliance starts protecting the VM with the same profile.

Both the ESX Server and the Virtual Appliance may try to look up the hostname of the Manager and not find it if the Manager is in a different DNS domain. You can solve this by renaming the Manager to its fully qualified domain name (FQDN). To rename the Manager, go to **System > System Information > System Activity**. Make sure **Network Map with Activity Graph** is selected, then click on the Manager in the Network Map to display the Manager's **Properties** window and edit the **Hostname** field to the FQDN.

The Virtual Appliance cannot perform Log Inspection or Integrity Monitoring because it is not running on the VM being protected. To perform Log Inspection or Integrity Monitoring on a VM, an in-guest Deep Security Agent must be installed.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Known Issues

For a list of known issues, please consult the latest release notes.

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Support

Please visit the Trend Micro customer support Web site for assistance with any of your Trend micro Products:

Trend Micro Customer Support

© Copyright 2011 Trend Micro Inc.
All rights reserved.

Legal Notice

"Trend Micro", "Deep Security Solutions", and the Trend Micro logo are trade-marks of Trend Micro, Inc. All other trade-marks are the property of their respective owners.

Protected by U.S. Patent No. 7,630,982 B2.

Privacy Policy

Trend Micro, Inc. is committed to protecting your privacy. Please read the Trend Micro Privacy Policy available at www.trendmicro.com.

© Copyright 2011 Trend Micro Inc.
All rights reserved.